(19)日本国特許庁（ＪＰ）　(12)**公表特許公報（Ａ）**　(11)特許出願公表番号
特表2003－527645
（P2003－527645A）
(43)公表日　平成15年９月16日(2003.9.16)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/00	５４５	Ｇ０６Ｆ　12/00	５４５Ｍ	５Ｂ０１７
	５３７		５３７Ｈ	５Ｂ０７５
1/00		12/14	３２０Ｂ	５Ｂ０７６
12/14	３２０	17/30	１１０Ｆ	５Ｂ０８２
17/30	１１０		１２０Ｂ	

審査請求　未請求　予備審査請求　有　（全 97 頁）　最終頁に続く

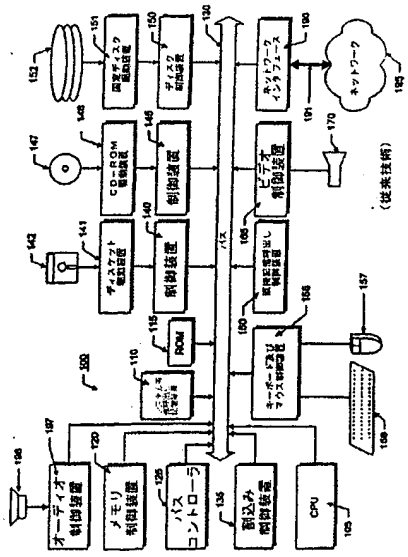
(21)出願番号　特願2000－583224(P2000－583224)
(86)(22)出願日　平成11年11月15日(1999.11.15)
(85)翻訳文提出日　平成13年５月16日(2001.5.16)
(86)国際出願番号　ＰＣＴ／ＵＳ９９／２７１１３
(87)国際公開番号　ＷＯ００／０３０３２３
(87)国際公開日　平成12年５月25日(2000.5.25)
(31)優先権主張番号　６０／１０８，６０２
(32)優先日　平成10年11月16日(1998.11.16)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／３１０，２９４
(32)優先日　平成11年５月12日(1999.5.12)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　イントゥー　ネットワークス　インク
アメリカ合衆国　マサチューセッツ州　02140　ケンブリッジ　ケンブリッジ　パーク　ドライブ　150
(72)発明者　シュマイドラー　ヨナー
アメリカ合衆国　マサチューセッツ州　02139　ケンブリッジ　ハーバード　ストリート　295
(72)発明者　アトキンス　デレック
アメリカ合衆国　マサチューセッツ州　02144　サマービル　ファーガット　アベニュー　6
(74)代理人　弁理士　金久保　勉

最終頁に続く

(54)【発明の名称】　広帯域アクセスネットワークを介してコンテンツを安全に引き渡すための方法及び装置

(57)【要約】
広帯域アクセスネットワークを介して、オンデマンドによってコンテンツを安全に引き渡すための方法は、クライアントプロセスで、承認なしにコンテンツを入手及び実行されないようにするために、１組のサーバと複数の安全機能を利用する。複数の暗号化されたタイトルが、このネットワークに接続されたコンテンツサーバに格納されている。同様にネットワークに接続されたアクセスサーバには、ネットワークアドレスと、上述のタイトルを暗号解読して実行するのに必要な種々のキーイング及び承認データが包含されている。ユーザのローカルコンピュータシステムで走るクライアントアプリケーションは、コンテンツサーバからタイトルを検索し且つユーザのローカルコンピュータシステムでタイトルを実行可能にする前に、アクセスサーバからアドレス、キーイング及び承認データを検索する必要がある。



【特許請求の範囲】

【請求項１】　ネットワークを介してコンテンツを引き渡すための方法であって、

（ａ）前記ネットワークに機能的に接続されたコンテンツサーバ上に少なくとも一つのタイトルを、実行不可能な形式で記憶する段階と、

（ｂ）前記ネットワークに機能的に接続されたアクセスサーバに、前記タイトルの位置識別子と前記タイトルを実行可能な形式に処理するのに必要なデータとを記憶する段階と、

（ｃ）前記コンテンツサーバから前記タイトルの少なくとも一部を検索する以前に、前記アクセスサーバから前記タイトルの前記位置識別子を入手することを、前記ネットワークに機能的に接続されたクライアントプロセスに要求する段階と、

（ｄ）前記タイトルの前記一部を実行可能な形式に処理するのに必要な前記データを、前記アクセスサーバから入手するように、クライアントプロセスに要求する段階と、を包含する方法。

【請求項２】　（ｅ）前記クライアントプロセスに、前記アクセスサーバの署名を入手すると共に、前記コンテンツサーバから前記タイトルの少なくとも一部を検索する前に前記コンテンツサーバにその署名を提示するよう要求する段階を更に包含する、請求項１に記載の方法。

【請求項３】　（ｅ）前記クライアントプロセスが前記コンテンツサーバから前記タイトル前記タイトルの少なくとも一部を検索可能な時間を定義する時間データを、前記アクセスサーバから入手するよう前記クライアントプロセスに要求する段階を更に包含する、請求項１に記載の方法。

【請求項４】　（ｆ）前記の時間が満期になった時点で且つ前記コンテンツサーバから前記タイトル前記タイトルの少なくとも一部を検索する前に、新しい時間データを前記アクセスサーバから入手するよう前記クライアントプロセスに要求する段階を更に包含する、請求項３に記載の方法。

【請求項５】　ネットワークを介してコンテンツを安全に引き渡すための装置であって、

（ａ）前記ネットワークに機能的に接続されると共に、少なくとも一つのタイトルを、実行不可能な形式で記憶してあるコンテンツサーバと、

（ｂ）前記ネットワークに機能的に接続されるアクセスサーバであって、前記タイトルの位置識別子と前記タイトルを実行可能な形式に処理するのに必要なデータとを記憶するアクセスサーバと、

（ｃ）前記ネットワークに機能的に接続されるクライアントシステムであって、前記タイトルの前記位置識別子と前記タイトルの前記一部を実行可能な形式に処理するのに必要な前記データとを、前記アクセスサーバから入手するように構成されたプログラムロジックを含んだクライアントシステムと、を包含する装置。

【請求項６】　前記クライアントシステムが、

前記タイトルの一部を実行するよう構成されたプログラムロジックを更に包含する、請求項５に記載の装置。

【請求項７】　前記アクセスサーバが、

前記タイトルの少なくとも一部を前記コンテンツサーバから検索可能な時間を定義する時間データを生成するように構成されたプログラムロジックを更に包含する、請求項５に記載の装置。

【請求項８】　前記クライアントシステムが、

前記の時間が満期になった時点で、新しい時間データを前記アクセスサーバから要求するように構成されたプログラムロジックを更に包含する、請求項７に記載の装置。

【請求項９】　前記ネットワークが広帯域アクセスネットワークを包含する、請求項５に記載の装置。

【請求項１０】　ネットワークを介してコンテンツを引き渡すための装置であって、

（Ａ）前記ネットワークに接続可能なコンテンツ・サーバシステムで、

（Ａ．１）時間間隔を特定するデータを含むと共にクライアントプロセスから受け取ったトークンに応答する認証プログラムロジックであって、前記クライアントプロセスが特定の時間にメモリにアクセスする許可を受けているか

どうかを判断するよう構成された認証プログラムロジックと、

（A．2）前記クライアントプロセスから受け取られる共に前記メモリに記憶されたタイトルの一つを固有に特定するデータを含んだ前記トークンに応答するアクセスプログラムロジックであって、前記メモリ及び前記トークンにより固有に特定された前記タイトルに対するアクセスを可能とするよう構成されたアクセスプログラムロジックとを包含した、コンテンツサーバシステムと、

（B）前記ネットワークに接続可能なアクセスサーバシステムであって、

（B．1）クライアントプロセスが提供したタイトルの固有識別子に応答する変換プログラムロジックであって、前記タイトルの前記固有識別子を、前記ネットワーク上の、前記タイトルにアクセス可能なアドレスを示す位置識別子に変換するよう構成されている変換プログラムロジックと、

（B．2）クライアントプロセスからの要求に応答するアクティベータ生成プログラムロジックであって、前記要求に応答してアクティベータを生成するアクティベータ生成プログラムロジックと、を包含するアクセスサーバシステムと、

（C）前記コンテンツサーバ及び前記アクセスサーバシステムに前記ネットワークを介して接続可能なクライアントシステムであって、

（C．1）前記アクセスサーバシステムから、トークンと、アクティベータと、特定されたタイトルにアクセスできる前記コンテンツサーバの位置識別子とを入手するよう構成されたプログラムロジックと、

（C．2）前記コンテンツサーバから前記特定されたタイトルの少なくとも一部を検索するよう構成されたプログラムロジックと、

（C．3）前記コンテンツサーバから検索された前記特定されたタイトルの前記一部を実行するよう構成されたプログラムロジックと、を包含するクライアントシステムと、

を包含する装置。

【請求項１１】　前記クライアントシステムが、そのシステム上で実行可能なオペレーティングシステムを更に包含し、更に、前記クライアントプロセスが、

（C．4）　前記特定されたタイトルに関連したネットワーク・ファイ

ルシステムをマウントすると共に、前記クライアントシステムのメモリに前記タイトルに関連した複数レジストリエントリを記憶するよう構成されたプログラムロジックと、

（C．５）タイトル実行中に前記オペレーティングシステムからの複数の要求を傍受すると共に、前記レジストリエントリに前記傍受した要求の選択部分を転送するよう構成されたプログラムロジックとを更に包含する、請求項１０に記載の装置。

【請求項１２】　前記アクティベータが暗号データを包含する、請求項１０に記載の装置。

【請求項１３】　前記アクティベータが少なくとも一つのバイトコードを包含し、更に、前記クライアントシステムが、

（C．４）前記アクティベータ内に含まれた前記バイトコードを解釈し且つ実行するプログラムロジックを包含する、請求項１０に記載の装置。

【請求項１４】　ローカルコンピュータシステム上のアプリケーションを、そのアプリケーションが前記ローカルコンピュータシステムにインストールされていなくても実行する方法であって、

（a）ネットワークマウント可能なファイルシステムと前記アプリケーションに関連した一組のレジストリエントリとにアクセスする段階と、

（b）前記ネットワークファイルシステムをマウントする段階と、

（c）前記レジストリエントリを前記ローカルコンピュータシステムに記憶する段階と、

（d）遠隔源から前記アプリケーションの少なくとも一部を検索する段階と、

（e）前記ローカルコンピュータシステムのオペレーティングシステムの制御下で前記アプリケーションを実行する段階と、

（f）前記オペレーティングシステムからの要求を傍受する段階と、

（g）前記傍受した要求の選択部分を、前記ローカルコンピュータシステムに記憶されたレジストリエントリに転送する段階とを包含した、アプリケーションの実行方法。

【請求項１５】　プロセッサと、メモリと、１つかそれ以上のアプリケーショ

ンを実行する能力を備えたオペレーティングシステムとを備えたコンピュータシステムにおいて、アプリケーションを前記コンピュータシステムにインストールしなくても実行するためのシステムであって、

ネットワークファイルシステムをマウントすると共に前記アプリケーションに関連した複数のレジストリエントリをメモリに記憶するように構成されたプログラムロジックと、

遠隔源から前記アプリケーションの少なくとも一部を検索するように構成されたプログラムロジックと、

前記オペレーティングシステムからの要求に応答するプログラムロジックであって、前記オペレーティングシステムからの要求を傍受すると共に前記傍受した要求の選択部分を前記レジストリエントリに転送するよう構成されたプログラムロジックとを包含する、アプリケーションを実行するためのシステム。

【請求項１６】　アクセスサーバと１つ又はそれ以上のタイトルデータソースにコンピュータネットワークを介して機能的に接続されたローカルコンピュータシステム上で実行されるクライアントプロセスにおいて、タイトルのオンデマンド引き渡しを可能とする方法であって、

（ａ）前記アクセスサーバからトークンと、アクティベータと、特定されたタイトルがアクセス可能なソースのネットワークアドレスとを入手する段階と、

（ｂ）前記トークンを前記ソースに送信する段階であって、このトークンデータが、前記ソースにアクセス可能な時間間隔を定義する、送信段階と、

（ｃ）前記ソースから前記タイトルの少なくとも一部を検索する段階と、

（ｄ）前記ソースから検索したタイトルの前記一部を実行する段階と、

（ｅ）前記アクセスサーバから更新されたトークンを入手する段階とを包含する、方法。

【請求項１７】　前記タイトルがネットワークマウント可能なファイルシステムと、一組のレジストリエントリとを包含し、更に、前記ステップ（ｄ）が、

ｄ１．前記ネットワークファイルシステムをマウントすると共に前記レジストリエントリ記憶する段階と、

ｄ２．前記ローカルコンピュータシステムで実行されているオペレーティング

システムからの要求を傍受すると共に前記傍受された要求の選択部分を前記レジストリエントリに転送する段階とを包含した、請求項９に記載の方法。

【請求項１８】　プロセッサと、メモリと、ネットワークインターフェースとを備えると共に、コンピュータネットワークに接続可能なサーバ装置において、要求プロセスによるタイトルへのアクセスを可能にする方法であって、

（ａ）要求プロセスからのランチストリングを認証する段階と、

（ｂ）要求プロセスから受け取ったタイトルの固有識別子を、このタイトルにアクセス可能な前記コンピュータネットワーク上のアドレスを示す位置識別子に変換する段階と、

（ｃ）アクティベータを生成する段階と、

（ｄ）前記アクティベータを前記コンピュータネットワークを介して前記要求プロセスに送る段階とを包含する、方法。

【請求項１９】　ロセッサと、メモリと、ネットワークインターフェースとを備えると共に、コンピュータネットワーク　１つかそれ以上のクライアントプロセスに接続可能なサーバ装置で用いる方法であって、

（ａ）クライアントプロセスから、一定時間を特定するデータとタイトルを固有に特定するデータとを含んだトークンを前記ネットワークインターフェースを介して受け取る段階と、

（ｂ）前記クライアントプロセスが特定の時間に前記タイトルにアクセスする許可を受けているかどうか判断する段階と、

（ｃ）前記段階（ｄ）において前記クライアントが許可されていれば、前記メモリと前記トークンにより固有に特定されているタイトルにアクセスする段階と、

（ｄ）前記トークンにより特定されている前記タイトルの少なくとも一部を前記クライアントに供給する段階とを含んだ、方法。

【請求項２０】　１つかそれ以上の要求者プロセスへのタイトルのコンピュータネットワークを介した選択的引き渡しを可能とするする方法であって、

（ａ）要求者プロセスに、前記コンピュータネットワーク上のアドレスに実行不可能な形式で記憶されているタイトルの選択した部分へのアクセスを所定の条

件で提供し、

（ｂ）前記要求者プロセスに、前記タイトルを実行不可能な形式からの実行可能な形式への処理に有用なデータを提供する段階と、

（ｃ）前記タイトルが前記コンピュータ上にインストールされるのを防止する一方で、前記コンピュータシステムにおける前記タイトルの選択した部分の実行を許容する段階とを包含した、方法。

【請求項２１】　タイトルをコンピュータネットワークを介して１つかそれ以上の要求者プロセスに引き渡す方法であって、

（ａ）要求者プロセスから、タイトルを特定するデータを受け取り、

（ｂ）前記要求者プロセスに、前記タイトルにアクセス可能な前記コンピュータネットワーク上の位置を特定するデータと前記タイトルにアクセスするのに必要な許可データとを提供する段階と、

（ｃ）前記要求者プロセスから支払い情報を受け取る段階とを包含した、方法。

【発明の詳細な説明】

【０００１】

関連出願

本願は、名称が「広帯域アクセスネットワークを介してコンテンツを安全に引き渡すための方法及び装置」であり、ヨナー・シュマイドラー等により、１９９８年９月１６日に出願された米国仮特許出願第６０／１０８６０２号に基づいて優先権を主張する。

【０００２】

更に、本願は、同一発明者であるヨナー・シュマイドラー等により出願された、３件の共同所有された米国特許出願に基づいて優先権を主張する。上記出願には、

【０００３】

名称が「広帯域アクセスネットワークを介してコンテンツを安全に引き渡すための方法及び装置」であり、ヨナー・シュマイドラー等により１９９９年５月１２日に出願された米国出願第０９／３１０２９４号、弁護士整理番号第Ａ００２８／７０００と、

【０００４】

名称が「コンテンツの安全な引き渡しシステムに於けるインストール抄録のための方法及び装置」であり、ヨナー・シュマイドラー等により１９９９年５月１２日に出願された米国出願第０９／３１１９２３号、弁護士整理番号第Ａ００２８／７００１と、

【０００５】

名称が「コンテンツの安全な引き渡しに於けるコンテンツ保護のための方法及び装置」という、ヨナー・シュマイドラー等により１９９９年５月１２日に出願された米国出願第０９／３１０２９９号、弁護士整理番号第Ａ００２８／７００２と、

【０００６】

名称が「広帯域アクセスネットワーク上でのオンデマンド配信のための方法及び装置」であり、ヨナー・シュマイドラー等により１９９９年５月１２日に出願

された米国出願第ＸＸ／ＸＸＸＸＸＸ号、弁護士整理番号第Ａ００２８／７００３とを包含する。

【０００７】

上記で特定した同時特許出願中の発明対象は、ここで参照することにより本明細書に編入される。

【０００８】

発明の分野

本発明は、一般的には、ネットワークを介してデータを分配するための方法及びシステムに関し、更に詳細には、実行可能なソフトウェアのコンテンツを、オン・ディマンド加入又は申込み（原語：subscription)が可能な態様で、広帯域アクセスネットワークを介して引き渡しするためのシステムに関する。

【０００９】

発明の背景

ソフトウェアアプリケーション及びオーディオ、ビデオ、アニメーション等のようなマルチメディアデータ型のオンデマンド引き渡しは、主にネットワークを介する送信速度のせいで、最近まで実用的ではなかった。一連のビットにフォーマットされるデータの送信速度は、ｂｐｓと呼ばれる。初期のモデムの情報伝達能力は、１秒当たり約３００ビットの送信速度であったが、その後モデムのデータ送受信速度が増大した。このようなモデム速度の増大につれて、ネットワークを介して送信されるデータの型ばかりでなくネットワークの接続形態の性質も進歩を始めた。９６００ｂｐｓ及び１２００ｂｐｓのモデム速度では、インターネットのようなコンピュータネットワークは、主に特定のプロトコルとテキストメッセージを有するアスキーテキスト環境であった。モデム速度が引き続き増大することで、より複合的な情報がインターネット及び他のコンピュータネットワークを介してアクセスできるようになった。今日依然として、アスキーテキストパラダイムが、インターネットのワールドワイドウェブ部分に残っているが、ごく最近の帯域幅環境の増大によって、更に複合的なコンテンツ及びマルチメディアデータ型の通信が可能になってきた。

【００１０】

最近では、１００万ｂｐｓを超える接続速度を有する高性能広帯域技術及びケーブルモデムが、ケーブル通信、電話通信、移動電話通信及び衛星通信企業によって世界中で展開且つ提供されつつある。現在の広帯域アクセスネットワークには、ケーブル通信産業の媒体共有型の複合ファイバー同軸ケーブル（ＨＦＣ）ネットワーク及び電話通信産業のデジタル加入者回線（ｘＤＳＬ）が含まれる。

【００１１】

広帯域技術及び広帯域アクセスネットワークの登場によって、以前には、コンパクトディスク読出し専用記憶素子（ＣＤ－ＲＯＭ）及びデジタル多目的ディスク（ＤＶＤ）でしか入手できなかった、複合的なマルチメディアデータ型及びソフトウェアタイトル（以後「タイトル」と呼ぶ）に、現在では、広帯域アクセスネットワークサービスの加入者が、遠隔地からアクセスすることができる。

【００１２】

しかし、データ送信速度以外にもタイトルのオンデマンド引き渡しの実用化を阻んできた要因がある。ソフトウェア及びマルチメディアタイトルを含むコンテンツのオンデマンド引き渡しを今日まで阻んできたそのような障害の１つは、タイトルを実行する上で、加入者のローカルコンピュータシステムにタイトルをロードさせるという必要性であった。更に、広範に行われているコンテンツの複製又は「海賊版製作」、及び全機能を備えたタイトルの複製の配信に伴う安全性に関わるリスクのために、オンデマンド配信は、ソフトウェア出版業者及びコンテンツライブラリにとって魅力的ではなかった。

【００１３】

よって、加入者のローカルコンピュータのシステムにインストールする必要のない、実行可能なソフトウェアコンテンツを、オンデマンドで引き渡すための方法及びシステムに対する必要性が存在する。

【００１４】

更に、コンテンツの価値を保護するセキュリティを提供し、且つその無断使用及び複製を防止するコンテンツを、加入者のローカルコンピュータのシステムに、オンデマンド引き渡しするための方法及びシステムに対する必要性が存在する。

【００１５】

更に、コンテンツ実行中の待ち時間要件を満足させる方法で、広帯域アクセスネットワークを介してコンテンツを引き渡すことができる方法及びシステムに対する必要性が存在する。

【００１６】

発明の概要

本発明の安全なコンテンツ引き渡しプラットホーム（ＳＣＤＰ）は、高帯域幅実行可能コンテンツを、オンデマンドで且つ広帯域アクセスネットワークを介して引き渡しを行う。このＳＣＤＰプラットホームを使用して、例えば、ケーブルモデム及びｘＤＳＬサービスの加入者のような広帯域加入者は、広帯域ネットワークを介してタイトルにアクセスできる。

【００１７】

ユーザは、例えば、入手可能なタイトルの仮想カタログを表示するワールドワイドウェブ上で、仮想店舗ショーウインドウから実行すべきタイトルを選択する。交渉には、第三者電子コマースシステム（Ｅコマース）にユーザ登録すること、タイトルを選択すると、ユーザはそのタイトルを実際に購入するために交渉する。ユーザ課金情報を提供すること及び選択タイトルに付随して提示される購入タイプの中から１つを選択することが含まれる。考えられる購入タイプの例としては、１）特定のタイトルの期限付き試用、２）任意のタイトルの「一回使用」毎の１回の支払い、３）週極め、月極め等の一定の具体的な期間に亘るタイトルの無制限の「複数使用回」を許可する１回の支払いがある。

【００１８】

購入交渉が完了すると、ユーザのパーソナルコンピュータで実行中のＳＣＤＰクライアントソフトウェアが、条件付きアクセスサーバ（ＣＡＳ）から、許可トークン及びキーイングデータを入手する。このトークンによって、クライアントプロセスは、広帯域ネットワークを介してアクセス可能なネットワークファイルサーバから選択したタイトルの実行を許可される。ファイルサーバから検索されたデータは暗号化される。ＳＣＤＰクライアントプロセスには、ファイルサーバからのデータを暗号解読するために、条件付きアクセスサーバによって提供され

るキーイングデータを使用する。本発明では、タイトルはユーザのパーソナルコンピュータで走るが、タイトルはそれの全体が、このパーソナルコンピュータにダウンロードされるわけではない。タイトルは電子的なパッケージの中にフォーマットされており、そのパッケージには、圧縮且つ暗号化された形式で、タイトルのファイルが含まれている（以後ｂｒｉｑと呼ぶ）。このｂｒｉｑは、実際には、ポータブルな、独立言語ファイルシステムであり、特定のタイトルを実行するのに必要なファイルが全て含まれている。ｂｒｉｑは、広帯域ネットワークを介してアクセス可能なネットワークファイルサーバ（以後ＲＡＦＴサーバと呼ぶ）に格納されている。ＳＣＤＰクライアントは、ｂｒｉｑを、ユーザのパーソナルコンピュータのローカルファイルシステムの如く取扱う。タイトルを実行する場合、例えばウィンドウズ（Ｒ）のようなオペレーティングシステムが、このようなローカルファイルシステムに読出しを要求する。図示された実施例では、ウィンドウズ（Ｒ）仮想デバイスドライバ（ＶｘＤ）を含むＳＣＤＰクライアントが、ＲＡＦＴサーバから、ｂｒｉｑデータの要求されたブロックを検索することによって、このような要求に応える。データの要求されたブロックを検索後、ＶｘＤが、ｂｒｉｑデータを圧縮且つ暗号化し、そのデータを、ユーザのパーソナルコンピュータのオペレーティングシステムに送る。

【００１９】

本発明の１つの態様によれば、ソフトウェアタイトルが、ターゲットコンピュータに「インストール」されることは決してない。ＳＣＤＰクライアントソフトウェアによって、１つのインストール抽象が創り出され、現在実行中のタイトルはホストコンピュータにインストールされている、という錯覚を、オペレーティングシステムに対して維持する。従って、タイトルの実行が終了すると、システム上にはタイトルが実行されたという形跡は何も残らない。タイトルに関連するファイルは、パーソナルコンピュータのハードディスクには何も残らず、更にタイトルに関連するレジストリ変数などのオペレーティングシステムの状態情報も一切残存しない。タイトルの利用者は、ゲームなどで獲得した「レベル」のような、プレイ全般に亘って維持することが望ましいと思われる、ある種の状態情報を保存するオプションを有する。このような状態情報は、後述のライトスルーフ

ァイルに保存できる。

【００２０】

本発明の別の態様によれば、ＳＣＤＰクライアントソフトウェアは、本発明の所有権を主張できるランダムアクセスファイル転送（ＲＡＦＴ）プロトコルを使用して、広帯域ネットワークを介してｂｒｉｑデータを検索する。このプロトコルは、ＳＣＤＰクライアントに、ＲＡＦＴサーバに格納されているファイル及びディレクトリへの読出し専用アクセスを提供する。ｂｒｉｑは１つのローカルファイルシステムとして取り扱われるので、ＲＡＦＴクライアントは、１つのオペレーティングシステムドライブとして存在が認識される必要が無く、又オペレーティングシステムのファイルシステムマネージャ、即ち図示された実施例におけるウィンドウズ（Ｒ）・インストラブル・ファイルシステム（ＩＦＳ）マネージャに、インターフェースをとる必要がない。従って、ＲＡＦＴクライアントファイルシステムドライバ、即ち図示された実施例におけるＶｘＤは、遠隔又はネットワークファイルシステムドライバよりも小さく、単純である。更に、ＲＡＦＴプロトコルは、「帯域幅スロットリング」のようなダイナミック帯域幅の制限をサポートし、又ＲＡＦＴ許可トークンの使用を通じてアクセス制御をサポートする。

【００２１】

本発明の別の態様によれば、ＳＣＤＰは、種々の安全機能を用いて、無断アクセス及びリプレイからコンテンツを保護する。許可トークン及び暗号解読キーは、条件付きアクセスサーバから入手する。ＳＣＤＰクライアントとＣＡＳ間のネットワーク通信は、安全な遠隔手続き呼出し（ＲＰＣ）インタフェースを介して保護される。一旦、安全チャネルがＳＣＤＰとＣＡＳ間で確立されると、ＳＣＤＰクライアントは、選択されたタイトルのＲＡＦＴ許可トークン及びキーイングデータを要求する。この許可トークンは、ＣＡＳからの符号化されたメッセージであり、それによって、要求を行っているユーザが、特定のｂｒｉｑに、特定のＲＡＦＴファイルサーバで、また交渉済みの支払タイプで明確にされた期間、アクセスできることを表す。

【００２２】

ＲＡＦＴ許可トークンによって、ＳＣＤＰクライアントがタイトルのｂｒｉｑへのアクセスを許されても、このＳＣＤＰクライアントは、タイトルのファイルデータへアクセスするのにｂｒｉｑを、例えば、圧縮解除及び暗号解読など更にアンパックしなければならない。ＣＡＳによって、ユーザはｂｒｉｑデータを暗号解読するのに必要なキーイングデータを提供されるが、ＣＡＳは、ＳＣＤＰクライアントにキーイングデータを直接提供するわけではない。直接提供する代わりに、ＣＡＳは、暗号解読アルゴリズムを実行する曖昧化したバイトコードにキーを埋込むことによって、キーイングデータをユーザから隠す。孤立したキーイングデータをＳＣＤＰクライアントに引き渡すのではなく、ＣＡＳは、曖昧化したバイトコード（以後アクティベータと呼ぶ）を引き渡す。ＳＣＤＰクライアントの仮想デバイスドライバが、バイトコード解釈プログラムでこのアクティベータを実行することで、ｂｒｉｑデータの暗号解読を行う。コード曖昧化によって、アクティベータを逆行分析するのが困難になり、ハッカーは、このアクティベータからキーイングデータを取り出すためには、かなりの時間と資源を費やさねばならなず、一般的には、そのコストは保護されているコンテンツの価値以上になる。本発明の意図するところでは、アクティベータは、１件のクライアント当たり、１つのｂｒｉｑ当たり、また１回の実行当たり只１つであり、即ち、ＣＡＳから入手されるアクティベータは、それぞれ異なっており、且つ只１回だけ使用可能である。そうすることで、複数回使用するユーザーに対して、１回ごとの、コストの掛かる逆行分析を行なおうとする気持ちにさせない。

【００２３】

本発明によれば、ＲＡＦＴ認証トークン及びアクティベータには、共に限られた寿命が設定されている。認証トークンには満了期間が含まれており、それ以後は無効となる。実行中のアクティベータは、一定の時点で、自己更新のためにＣＡＳと交換を開始する。その交換に失敗すると、アクティベータが動作不能になり、従ってタイトルは動作不能になる。アクティベータの更新を、以後、アクティベータ保持と呼ぶ。この保持機能の結果、現在実行中のアクティベータに、新たなキー、データ又はコードすらも含みうる最新版が引き渡されることになる。認証トークンが更新されるとアクティベータも更新される。新たな認証トークン

は、暗号解読用キーイングデータと一緒に、この新たなアクティベータ内に埋込まれる。始動時に、更新アクティベータが、ＳＣＤＰクライアント内のＲＡＦＴ・ＶｘＤへ新たなＲＡＦＴ認証トークンを引き渡す。

【００２４】

ＳＣＤＰシステムは媒体非依存であり、ユーザとネットワークサーバ間に、現在実行中のＣＤタイトルの時間要件を満足させるのに十分な帯域幅が存在していれば、ＨＦＣネットワーク及び電話企業のデジタル加入者回線を含む、任意の広帯域ネットワーク技術全般で動作するものである。またＳＣＤＰシステムは、１０メガｂｐｓ及び１００メガｂｐｓのイーサネット（Ｒ）・ローカルエリアネットワークを使用しても実現でき、例えば、同じようにイントラネットを介して実行可能なコンテンツを引き渡すための企業ネットワーク内でも実行できる。

【００２５】

本発明の第１の実施例によれば、ネットワークを介してコンテンツを引き渡すための方法が、（ａ）前記ネットワークに機能的に接続されたコンテンツサーバ上に少なくとも一つのタイトルを、実行不可能な形式で記憶する段階と、（ｂ）前記ネットワークに機能的に接続されたアクセスサーバに、前記タイトルの位置識別子と前記タイトルを実行可能な形式に処理するのに必要なデータとを記憶する段階と、（ｃ）前記コンテンツサーバから前記タイトルの少なくとも一部を検索する以前に、前記アクセスサーバから前記タイトルの前記位置識別子を入手することを、前記ネットワークに機能的に接続されたクライアントプロセスに要求する段階と、（ｄ）前記タイトルの前記一部を実行可能な形式に処理するのに必要な前記データを、前記アクセスサーバから入手するように、クライアントプロセスに要求する段階と、を包含する。

【００２６】

本発明の第２の実施例によれば、ネットワークを介してコンテンツを安全に引き渡すための装置が、（ａ）前記ネットワークに機能的に接続されると共に、少なくとも一つのタイトルを、実行不可能な形式で記憶してあるコンテンツサーバと、（ｂ）前記ネットワークに機能的に接続されるアクセスサーバであって、前記タイトルの位置識別子と前記タイトルを実行可能な形式に処理するのに必要な

データとを記憶するアクセスサーバと、（c）前記ネットワークに機能的に接続されるクライアントシステムであって、前記タイトルの前記位置識別子と前記タイトルの前記一部を実行可能な形式に処理するのに必要な前記データとを、前記アクセスサーバから入手するように構成されたプログラムロジックを含んだクライアントシステムと、を包含する。

【００２７】

本発明の第３の実施例によれば、ネットワークを介してコンテンツを引き渡すための装置が、（A）前記ネットワークに接続可能なコンテンツ・サーバシステムであって、（A．１）時間間隔を特定するデータを含むと共にクライアントプロセスから受け取ったトークンに応答する認証ロジックであって、前記クライアントプロセスが特定の時間にメモリにアクセスする許可を受けているかどうかを判断する認証ロジックと、（A．２）前記クライアントプロセスから受け取られる共に前記メモリに記憶されたタイトルの一つを固有に特定するデータを含んだ前記トークンに応答するアクセスプログラムロジックであって、前記メモリ及び前記トークンにより固有に特定された前記タイトルに対するアクセスを可能とするアクセスプログラムロジックとを包含した、コンテンツサーバシステムと、（B）前記ネットワークに接続可能なアクセスサーバシステムであって、（B．１）クライアントプロセスが提供したタイトルの固有識別子に応答する変換プログラムロジックであって、前記タイトルの前記固有識別子を、前記ネットワーク上の、前記タイトルにアクセス可能なアドレスを示す位置識別子に変換するよう構成されている変換プログラムロジックと、（B．２）クライアントプロセスからの要求に応答するアクティベータ生成ロジックであって、前記要求に応答してアクティベータを生成するアクティベータ生成ロジックと、を包含するアクセスサーバシステムと、（C）前記ネットワークに接続可能なクライアントシステムであって、（C．１）前記アクセスサーバシステムから、トークンと、アクティベータと、特定されたタイトルにアクセスできる前記コンテンツサーバの位置識別子とを入手するよう構成されたプログラムロジックと、（C．２）前記コンテンツサーバから前記特定されたタイトルの少なくとも一部を検索するよう構成されたプログラムロジックと、（C．３）前記コンテンツサーバから検索された前

記タイトルの前記一部を実行するよう構成されたプログラムロジックと、を包含するクライアントシステムと、を包含する。

【００２８】

本発明の第４の実施例によれば、ローカルコンピュータシステム上のアプリケーションを、そのアプリケーションが前記ローカルコンピュータシステムにインストールされていなくても実行する方法が、（ａ）ネットワークマウント可能なファイルシステムと前記アプリケーションに関連した一組のレジストリエントリとにアクセスする段階と、（ｂ）前記ネットワークファイルシステムをマウントする段階と、（ｃ）前記レジストリエントリを前記ローカルコンピュータシステムに記憶する段階と、（ｄ）遠隔源から前記アプリケーションの少なくとも一部を検索する段階と、（ｅ）前記ローカルコンピュータシステムのオペレーティングシステムの制御下で前記アプリケーションを実行する段階と、（ｆ）前記オペレーティングシステムからの要求を傍受する段階と、（ｇ）前記傍受した要求の選択部分を、前記ローカルコンピュータシステムに記憶されたレジストリエントリに転送する段階とを包含する。

【００２９】

本発明の第５の実施例によれば、アプリケーションをコンピュータシステムにインストールしなくても実行するためのシステムが、ネットワークファイルシステムをマウントすると共に前記アプリケーションに関連した複数のレジストリエントリをメモリに記憶するように構成されたプログラムロジックと、遠隔源から前記アプリケーションの少なくとも一部を検索するように構成されたプログラムロジックと、前記オペレーティングシステムからの要求に応答するプログラムロジックであって、前記オペレーティングシステムからの要求を傍受すると共に前記傍受した要求の選択部分を前記レジストリエントリに転送するよう構成されたプログラムロジックとを包含する。

【００３０】

本発明の第６の実施例によれば、タイトルのオンデマンド引き渡しを可能とする方法が、（ａ）前記アクセスサーバからトークンと、アクティベータと、特定されたタイトルがアクセス可能なソースのネットワークアドレスとを入手する段

階と、（ｂ）前記トークンを前記ソースに送信する段階であって、このトークンデータが、前記ソースにアクセス可能な時間間隔を定義する、送信段階と、（ｃ）前記ソースから前記タイトルの少なくとも一部を検索する段階と、（ｄ）前記ソースから検索したタイトルの前記一部を実行する段階と、（ｅ）前記アクセスサーバから更新されたトークンを入手する段階とを包含する。

【００３１】

本発明の第７の実施例によれば、要求プロセスによるタイトルへのアクセスを可能にする方法が、（ａ）要求プロセスからのランチストリングを認証する段階と、（ｂ）要求プロセスから受け取ったタイトルの固有識別子を、このタイトルにアクセス可能な前記コンピュータネットワーク上のアドレスを示す位置識別子に変換する段階と、（ｃ）アクティベータを生成する段階と、（ｄ）前記アクティベータを前記コンピュータネットワークを介して前記要求プロセスに送る段階とを包含する。

【００３２】

本発明の第８の実施例によれば、ロセッサと、メモリと、ネットワークインターフェースとを備えると共に、コンピュータネットワーク　１つかそれ以上のクライアントプロセスに接続可能なサーバ装置で用いる方法が、（ａ）クライアントプロセスから、一定時間を特定するデータとタイトルを固有に特定するデータとを含んだトークンを前記ネットワークインターフェースを介して受け取る段階と、（ｂ）前記クライアントプロセスが特定の時間に前記タイトルにアクセスする許可を受けているかどうか判断する段階と、（ｃ）前記段階（ｄ）において前記クライアントが許可されていれば、前記メモリと前記トークンにより固有に特定されているタイトルにアクセスする段階と、（ｄ）前記トークンにより特定されている前記タイトルの少なくとも一部を前記クライアントに供給する段階とを含んでいる。

【００３３】

本発明の第９の実施例によれば、１つかそれ以上の要求者プロセスへのタイトルのコンピュータネットワークを介した選択的引き渡しを可能とするする方法が、（ａ）要求者プロセスに、前記コンピュータネットワーク上のアドレスに実行

不可能な形式で記憶されているタイトルの選択した部分へのアクセスを所定の条件で提供し、（ｂ）前記要求者プロセスに、前記タイトルを実行不可能な形式からの実行可能な形式への処理に有用なデータを提供する段階と、（ｃ）前記タイトルが前記コンピュータ上にインストールされるのを防止する一方で、前記コンピュータシステムにおける前記タイトルの選択した部分の実行を許容する段階とを包含する。

【００３４】

本発明の第１０番目の実施例によれば、タイトルをコンピュータネットワークを介して１つかそれ以上の要求者プロセスに引き渡す方法が、（ａ）要求者プロセスから、タイトルを特定するデータを受け取り、（ｂ）前記要求者プロセスに、前記タイトルにアクセス可能な前記コンピュータネットワーク上の位置を特定するデータと前記タイトルにアクセスするのに必要な許可データとを提供する段階と、（ｃ）前記要求者プロセスから支払い情報を受け取る段階とを包含する。

【００３５】

本発明の第１１番目の実施例によれば、コンピュータネットワークを介して１つかそれ以上の要求者プロセスへ機能的に接続されたコンピュータシステムで使用されるコンピュータプログラム製品が、

（ａ）前記ネットワークに接続された要求者プロセスから選択したタイトルを特定するデータを検索するよう構成されたプログラムコードと、（ｂ）前記要求者プロセスから支払い情報を受け取るよう構成されたプログラムコードと、（ｃ）前記要求者プロセスが、前記タイトルの選択した部分にアクセスしてダウンロードするのを可能にするよう構成されたプログラムコードと、（ｄ）前記タイトルがコンピュータシステム上での実行は許容する一方、前記タイトルの前記コンピュータシステムへのインストールは防止するよう構成されたプログラムコードと、を包含する。

【００３６】

実施例の詳細な説明

図１に示すのは、カリフォルニア州パロアルトのサン・マイクロシステムズ社から市販されているサンスパークステーション５ワークステーション又はニュー

ヨーク州アーモックのインターナショナル・ビジネス・マシーンズ社から共に市販されているＩＢＭ　ＲＳ／６０００ワークステーション又はＩＢＭアプティバ・パーソナルコンピュータのようなコンピュータシステム１００用のシステムアーキテクチャであり、このようなアーキテクチャ上で本発明を実施することができる。図１のコンピュータシステムは、説明目的の例示にすぎない。この説明で、特定のコンピュータシステムを説明する際に共通して使われる用語に言及する場合があるが、本説明及び概念は、図１と異なるアーキテクチャを有するシステムを含め、他のシステムにも等しく該当する。

【００３７】

コンピュータシステム１００は、従来のマイクロプロセッサを用いて実行可能な中央演算処理装置（ＣＰＵ）１０５、情報の一時記憶用のランダムアクセスメモリ（ＲＡＭ）１１０及び情報の永久記憶用の読出し専用記憶素子（ＲＯＭ）１１５を包含する。メモリ制御装置１２０は、ＲＡＭ１１０を制御するために配設されている。

【００３８】

バス１３０は、コンピュータシステム１００の構成要素を相互接続する。バスコントローラ１２５は、バス１３０を制御するために配設されている。割込み制御装置１３５は、システム構成要素からの種々の割込み信号を受信及び処理するために用いられる。

【００３９】

大容量記憶装置は、ディスケット１４２、ＣＤ－ＲＯＭ１４７又はハードドライブ１５２であってもよい。データ及びソフトウェアは、ディスケット１４２及びＣＤ－ＲＯＭ１４７のような取外し可能な媒体を介して、コンピュータシステム１００とやり取り可能である。ディスケット１４２は、ディスケット駆動装置１４１へ挿入可能であり、その駆動装置は制御装置１４０を介して、更にバス３０に接続している。同様に、ＣＤ－ＲＯＭ１４７は、ＣＤ－ＲＯＭ駆動装置１４６へ挿入可能であり、その駆動装置は制御装置１４５を介して、更にバス１３０に接続している。ハードディスク１５２は、制御装置１５０を介してバス１３０に接続されている固定ディスク駆動装置１５１の一部をなす。

【００４０】

コンピュータ１００へのユーザ入力には、複数の装置がなりうる。例えば、キーボード１５６及びマウス１５７が、制御装置１５５を介してバス１３０に接続されている。マイクロホンとしても又スピーカとしても動作可能なオーディオトランジューサ１９６が、図に示すように、オーディオ制御装置１９７を介してバス１３０に接続されている。ペン及び／又はタブロイドのようなその他の入力装置が、必要であればバス１３０及び適切な制御装置やソフトウェアに接続されうることは、通常の技能を備えた当業者には明らかであろう。ＤＭＡ制御装置が、ＲＡＭに対して直接記憶呼出しを実行するために配設されている。視覚的表示は、ビデオ表示装置１７０を制御するビデオ制御装置１６５によって生成される。コンピュータシステム１００には、バス１９１及びネットワーク１９５によって概略的に示されているように、このコンピュータシステムがローカルエリアネットワーク（ＬＡＮ）又は広域ネットワーク（ＷＡＮ）と相互接続するを可能にする通信アダプタ１９０も包含されている。

【００４１】

コンピュータシステム１００の動作は、ワシントン州レドモンドのマイクロソフト社から市販されているウィンドウズ（Ｒ）９５又はウィンドウズ（Ｒ）ＮＴのようなオペレーティングシステムソフトウェアによって全体的に制御及び調整される。このオペレーティングシステムは、システム資源の割付けを制御し更に、とりわけ、処理スケジュール、記憶域管理、ネットワーキング及び出入力サービスのようなタスクを実行する。特に、システム記憶装置に常駐し、ＣＰＵ１０５で走るオペレーティングシステムは、コンピュータシステム１００のその他の構成要素の動作を調整する。本発明は、ＯＳ／２（登録商標）、ＵＮＩＸ（Ｒ）、Ｌｉｎｕｘ及びＳｏｌａｒｉｓ（登録商標）を含む任意の数の市販されているオペレーティングシステムを用いて実行してもよい。ネットスケープ・コミュニケーションズ社から市販のネットスケープナビゲータのバージョン２．０以上及びワシントン州レドモンドのマイクロソフト社から市販のインターネットエクスプローラのバージョン１．０以上等の１つ又はそれ以上のブラウザアプリケーションが、これらのオペレーションシステムの制御下で実行できる。

【００４２】

ＳＣＤＰシステムの概説

図２Ａに概念的に図示されているのは、本発明による安全なコンテンツ引き渡しプラットホーム（ＳＣＤＰ）システム２００及び広帯域ネットワーク環境におけるその他の要素であり、このような環境は例示目的のためにすぎず限定を意図したものではない。図２Ａに示す要素によって、本発明が簡便化され且つ理解されるはずである。図２Ａで示されたり、又はここに説明されている要素は、本発明の実施又は動作にとって必ずしも全てが必要であるわけではない。図２Ａに示す如く、ＳＣＤＰシステム２００は、条件付きアクセスサーバ（ＣＡＳ）２１０、付随のＣＡＳデータベース２１２、ランダムアクセスファイル転送サーバ（ＲＡＦＴ）２０６、ＲＡＦＴデータベース２０８及びＳＣＤＰクライアント２１６を包含する。

【００４３】

ＣＡＳサーバ２１０、ＲＡＦＴサーバ２０６及びＳＣＤＰクライアント２１６に加えて、本発明は、仮想店舗ショーウインドウ２１５及びＥコマースサーバ２０２の使用を意図している。Ｅコマースサーバ２０２は、付随する課金データベース２０４を有する。店舗ショーウインドウ２１５は、付随するデータベース２１３を有する。例示の実施例では、サーバ２０２、２１０及び２１５が、ローカルイーサネット（Ｒ）ネットワークのような、専用の、安全なローカルエリアネットワーク（ＬＡＮ）を介して接続されている。そのＬＡＮは更に、インターネットサービスプロバイダ（ＩＳＰ）２３０を介して、図２Ａのインターネットクラウド２４０として示されているように、広域コンピュータネットワークトポロジに接続されている。ＭＣＩ・ＷｏｒｌｄＣｏｍ、ＡＴ＆Ｔ、アメリカオンライン等の任意の商業利用可能なインターネットアクセスサービスプロバイダを、ＩＳＰ２３０として使用してもよい。例示の実施例では、サーバ２０２，２１０及び２１５が、専用ローカルエリアネットワークを介して接続されているものとして示してあるが、このようなサーバは、インターネットのような他の非専用ネットワークを介して機能的に接続されてもよいことは、当業者には明らかであろう。更に、Ｅコマースサーバ２０２が、金融又は銀行機関（図示せず）のクレジッ

ト取扱いサーバに接続されることで、クレジットカード及び／又は別種の取引の取扱いを促進する。

【００４４】

再び図２Ａを参照すると、図１と同様のアーキテクチャを有する、１つ又はそれ以上のクライアントパーソナルコンピュータが、広帯域アクセスネットワーク２０３及びケーブルプロバイダ２０７を介してＳＣＤＰシステム２００に接続されている。例示の実施例では、ケーブルモデム（ＣＭ）は、ＳＣＤＰクライアントが実行しているホストコンピュータに接続する。次いで、複数のケーブルモデムが、高周波接続を経由してケーブルノードに連結されている。一般的には、１０００ものホストパーソナルコンピュータが、適切なケーブルモデム及び高周波接続を介して１つのケーブルノードに接続しうる。各ケーブルノードは、更にケーブルモデム終端システム（ＣＭＴＳ）を介して終端ヘッドエンドに接続されている。複数のケーブルモデムが、１つの終端ヘッドエンドに接続されている。複数の相互接続されたヘッドエンドは、広帯域アクセスネットワークの中枢を構成する。これらのケーブルヘッドエンドは、ケーブル会社の施設に配置されているのが一般的であり、更にＴ１回線又は別の接続を介して、インターネットプロトコル（ＩＰ）ネットワークに接続されているホストデータ端末装置を含んでもよい。このＴ１回線は、更にインターネットサービスプロバイダ（ＩＳＰ）２３０を介してインターネットに接続されうる。ＲＡＦＴサーバ２０６及びそれに付随するデータベース２０８が、インターネットサービスプロバイダ２３０と、ケーブル会社が提供するホストデータ終端施設又はヘッドエンドとの間で、広帯域アクセスネットワーク２０３に接続されている。このようにして、ＲＡＦＴサーバ２０６は、ＳＣＤＰシステム２００の一部をなすが、ＣＡＳ２１０、Ｅコマースサーバ２０２及び仮想店舗ショーウインドウ２１５から遠隔配置されている。ケーブルモデム終端システム２０９は、ケーブル通信施設からの高周波データを、公開されているケーブル経由データサービス工業規格（ＤＯＣＳＩＳ）を適用して、インターネットプロトコルフォーマットに変換する。

【００４５】

或いは、図２Ａで示すように、クライアント・パーソナルコンピュータを、デ

ジタル加入者回線（ＤＳＬ）経由で、ＳＣＤＰシステム２００に接続してもよい。このような構成では、ＳＣＤＰクライアントが実行されているホストコンピュータは、ＤＳＬモデム及び既存の一般の交換電話回線施設を経由して電話会社のスイッチと接続される。

【００４６】

ＤＳＬ加入者ネットワーク及び広帯域アクセスネットワークの構造は、本発明の分野では公知であり且つケーブル会社及び電話会社によって現在広範に使用されているので、簡略のために此処ではこれ以上詳しく説明することは控えたい。よって、必ずしも上記説明のシステムの全要素が図２Ａで示されているわけではない。

【００４７】

加入手順

図２Ｂは、ＳＣＤＰシステム２００内の構成要素の相互作用を概念的に示したものである。図４Ａ乃至４Ｂのフローチャートは図２Ｂの概念ブロック図と合わせて、加入処理及びランチ（原語：launch）処理中にＳＣＤＰシステム２００が実行する本発明による処理ステップを示す。

【００４８】

パーソナルコンピュータ上でネットスケープ・ナビゲータ又はマイクロソフト・インターネットエキスプローラのようなＨＴＭＬブラウザを実行中のＳＣＤＰクライアント２１６を使用しているユーザは、ステップ４０１に示したように仮想店舗ショーウインドウ２１５からタイトルを選択する。店舗ショーウインドウ２１５では、入手可能な各タイトルは、汎用資源ロケータ（ＵＲＬ）内部に埋め込まれたデジタルオッファーとして表示してある。このデジタルオッファーは選択したタイトル及び購入タイプを特定する情報を含んでいる。ステップ４０２に示したように、デジタルオッファーを選択すると、加入者のブラウザをＥコマースサーバ２０２のＨＴＴＰフロントエンド２０２Ａに送る。ステップ４０３に示したように、ユーザは、デジタルオッファーＵＲＬ内の情報に基づきＥコマースサーバ２０２と購入交渉する。この交渉にはユーザ登録とクレジット情報の提供が通常含まれる。

【００４９】

ステップ４０４Ａに示したように、Ｅコマースサーバは、購入を特定し且つ許可する情報を含んだランチストリングを生成する。この情報には所望のコンテンツを固有に特定する汎用資源名（ＵＲＮ）が含まれる。このＵＲＮ及びランチストリングの形式及び記述は後に説明する。ステップ４０４Ｂに示したように、ランチストリングは、ＣＡＳ２１０によってデジタル署名され、ＳＣＤＰクライアント２１６に送達するためにＥコマースサーバ２０２に送信される。

【００５０】

ランチストリングは、ＭＩＭＥ（多目的インターネットメッセージ拡張仕様）ヘッダでパックされている。ステップ４０５に示したように、ランチストリングがＳＣＤＰクライアントのブラウザ２２４に受け取られると、ランチストリングに関連付けられたＭＩＭＥタイプをレジストリエントリ内に探し出し、その結果としてＳＣＤＰクライアント２１６内部のランチャモジュール２２０が呼び出されることになる。ステップ４０６Ａに示したように、ランチャ２２０はＣＡＳ２１０と安全な接続を確立して、ＣＡＳが指定したＵＲＮのＵＲＬを提供するように、つまりＵＲＮからＵＲＬへの変換を要求する。ＵＲＬは該当するｂｒｉｑデータの位置を特定する。ＣＡＳ２１０は該当するＵＲＬをランチャ２２０に送る。ステップ４０６Ｂに示したように、一旦ランチャは対応するｂｒｉｑデータの位置を特定すると、ランチストリングを含んだ購入要求をＣＡＳに送る。

【００５１】

ステップ４０７に示したように、ＣＡＳはランチストリングの署名を確認して、ＲＡＦＴ許可トークン及びアクティベータをランチャに返す。アクティベータ及び許可トークンは後に詳しく説明する。許可トークンはアクティベータ内部に埋め込まれていてもよい。次に、ステップ４０８に示したように、ランチャはアクティベータをＡＲＦＳＤ・ＶｘＤ２１８に渡すことでタイトルをランチする。ＡＲＦＳＤ・ＶｘＤはアクティベータを実行し、ＲＡＦＴ許可トークンをＲＡＦＴ・ＶｘＤ２２２に回す。ステップ４０９に示したようにＲＡＦＴ・ＶｘＤはＵＲＬを開けてヘッダを読む。ＲＡＦＴ・ＶｘＤ２２２は、ステップ４１０に示したように最初の許可トークンをＲＡＦＴサーバに送る。ステップ４１１に示した

ように、ＲＡＦＴ・ＶｘＤ２２２はＲＡＦＴサーバ２０６からのコンテンツを読み始め、受け取ったコンテンツをＡＲＦＳＤ・ＶｘＤ２１８に戻す。ステップ４１２に示したように、ＡＲＦＳＤ・ＶｘＤは、アクティベータを用いてｂｒｉｑデータ形式のコンテンツを解読及び復元解凍し、更に、解読データのブロックに保全性チェックを行う。

【００５２】

その後、ステップ４１３に示したように、オペレーティングシステムはＡＲＦＳＤ　ＶｘＤが提供するローカルファイルシステムを介してタイトルを実行する。アクティベータはランチャ２２０に対し定期的に要求して、ＣＡＳ２１０にアクティベータ及びＲＡＦＴ許可トークンを更新させる。ステップ４１４に示したように、最初の要求が出されると、ＣＡＳは購入をＥコマースサーバ２０２に通知して、取引が成立つまり完了する。最初のアクティベータの寿命は数分程度の場合もある。第１回目のタイムアウト後に正しくアクティベータが更新されると、このタイトルがうまく実行されていることを示す。

【００５３】

システム構成要素及びそれらの相互作用の大筋をこうして説明したところで、本発明の安全なコンテンツ引渡しシステム２００及びそこで実行される処理を図３Ａ乃至１４を参照して説明する。

【００５４】

ＳＣＤＰクライアント

図３Ａを参照すると、本発明によるＳＣＤＰクライアント２１６の概念ブロック図を示す。ＳＣＤＰクライアント２１６により、ユーザはホスト・パーソナルコンピュータ上でｂｒｉｑ符号化されたタイトルを実行できる。図３Ａに示したように、ＳＣＤＰクライアントは、ランチャ２２０、アレパ・ファイルシステム・ドライバＶｘＤ（ＡＲＦＳＤ・ＶｘＤ）２１８、及びＲＡＦＴクライアントＶｘＤ２２２を包含する。ＳＣＤＰクライアント２１６は、オペレーティングシステム２１９（例えば、本実施例ではウィンドウズ（Ｒ）アプリケーション）上を実行可能なアプリケーションとして実現してもよい。図１を参照して説明したように、オペレーティングシステム２１９はＩＢＭ・ＰＣ又はその他のコンピュー

タ・アーキテクチャのようなパーソナルコンピュータ・アーキテクチャ上で実行可能である。ＳＣＤＰクライアント２１６に加え、ブラウザ２１７（一般的にはネットスケープナビゲータ又はマイクロソフト・エキスプローラなどのＨＴＭＬブラウザ）は、オペレーティングシステム２１９の制御下に実行してもよい。ランチャ２２０、ＡＲＦＳＤ・ＶｘＤ２１８及びＲＡＦＴ・ＶｘＤ２２２は、後に図３Ｂ乃至３Ｄをそれぞれ参照してより詳しく説明する。

【００５５】

図３Ｂは、ＳＣＤＰクライアント２１６のランチャ２２０を包含するプログラムロジックモジュールのブロック図を概念的に示す。具体的には、ランチャ２２０は、制御モジュール３００、ＣＡＳ・ＲＰＣライブラリ３０２、ＡＲＦＳＤ・ＶｘＤ通信ライブラリ３０４、及びユーザインターフェース３０６を包含する。図示した実施例では、ランチャ２２０はＳＣＤＰクライアントとＣＡＳ２０４との間の全ての通信を調整するロジックを含んだウィンドウズ（Ｒ）・アプリケーションとして実現してもよい。Ｅコマースシステム２０２との購入交渉が完了すると、ランチャ２２０はクライアントのウェブブラウザ２１７に呼び出される。Ｅコマースシステムは、クライアント・ウェブサーバにランチャに関連したＭＩＭＥタイプ付きのランチストリングを送る。更に、ランチャはＣＡＳとの全ての通信を管理するが、その通信には１）ＣＡＳからのＲＡＦＴサーバのアドレス及び選択したタイトルに対応するｂｒｉｑパス名を入手、２）ＲＡＦＴサーバからｂｒｉｑデータを検索し、検索したデータを解読するのに必要なＲＡＦＴ許可トークン及びアクティベータのＣＡＳからの入手、及び３）ＲＡＦＴ許可トークン及びアクティベータをＣＡＳに対して更新依頼することが含まれる。

【００５６】

ＣＡＳサーバ２０６とＡＲＦＳＤ・ＶｘＤモジュール２１８との間の通信を容易にするため、ランチャ２２０は、ＣＡＳ・ＰＲＣライブラリ３０２を含む。このライブラリは遠隔手続き呼出し（ＲＰＣ）ライブラリを介してＣＡＳサーバ２０６との間で通信を行う一連のオブジェクト又はプログラムコードとして実現できる。モジュール３０２に適したＲＰＣライブラリとしては、ノーブルネット社から市販されているノーブルネット安全ＲＰＣプロダクトがある。オプションで

、ネットスケープ・コミュニケーションズ社が発行した安全ソケットライブラリ（ＳＳＬ）規格に準拠したネットワーク移送製品を用いて、ＲＰＣ呼び出しをネットワーク上で移送して、本発明のシステム内のＳＣＤＰクライアントとの通信安全性を向上させてもよい。通信ライブラリを、ランチャ・モジュール２２０とＡＲＦＳＤ・ＶｘＤモジュール２１８との間の通信と、ＡＲＦＳＤ・ＶｘＤモジュール２１８とＲＡＦＴクライアントＶｘＤ２２２との間の通信に用いてもよい。こうしたライブラリは、ランチャ２２０とＶｘＤ２１８とのデータ通信に必要なコード又はオブジェクトを含んでいてもよい。例えば、後に詳しく説明するように、ｂｒｉｑ１２００のｂｒｉｑヘッダ１２０２は、図１２に示すように、タイトルを実行中に制御モジュール３００によって読まれ、通信ライブラリ３０４を介してＶｘＤ２１８に提供される。

【００５７】

ランチャ２２０を呼び出すと、グラフィック・ユーザインターフェース（ＧＵＩ）がユーザインターフェース３０６を介してユーザに表示される。図示した実施例では、ユーザインターフェース３０６は、ウィンドウを作成し、そうしたウィンドウ内でグラフィック情報を表示し、キーボート、マウス、その他の位置決め装置を介してユーザからコマンドを受けるためにウィンドウズ（Ｒ）・オペレーティングシステムに含まれたオペレーティングシステム・インターフェース及びアプリケーションプログラム・インターフェース（ＡＰＩ）とのインターフェースをとるため適切なプログラムロジック及び／又はオブジェクトを含む。また、こうしたユーザインターフェースは通常の技能を備えた当業者の理解範囲に十分はいるものである。このＧＵＩを介して、ユーザはディスク・キャッシュサイズなどのユーザの好む設定を行うことができ、エラー状態も通知される。

【００５８】

制御モジュール３００は、タイトルをランチすると共にＳＣＤＰクライアント２００とＣＡＳ２１０とＲＡＦＴサーバ２０６との間の通信を継続するのに必要なアルゴリズムを実行するのに適したコード又はオブジェクトで実現できる。更に具体的には、制御モジュール３００が実行するアルゴリズムは図４Ａ乃至６及び関連した本明細書箇所により詳細に説明してある。

【００５９】

図３Ｃは、図３ＢのＡＲＦＳＤ・ＶｘＤ３０４の概念的ブロック図である。ＶｘＤ３０４は、バイトコード・インタプリタ３０８、制御モジュール３０４、及びＡＲＦＳＤ・ＶｘＤ通信ライブラリ３１２を包含する。ＡＲＦＳＤ・ＶｘＤ３０４は仮想デバイスドライバであり、オペレーティングシステムがｂｒｉｑデータをローカルファイルシステムとして読めるようにする。ＡＲＦＳＤ・ＶｘＤ３０４はｂｒｉｑデータを解凍解除及び解読する。更に、ＡＲＦＳＤ・ＶｘＤは、例えばウィンドウズ（Ｒ）・レジストリエントリを提供するなどインストール抄録（言語：abstract）を保持する。ＡＲＦＳＤ・ＶｘＤはオペレーティングシステムのアクセス呼び出しを全て傍受し且つ実行中だがディスクに保存はされないタイトルに関連したレジストリエントリをシミュレートして、動的レジストリエントリを実現する。

【００６０】

アクティベータ及びバイトコード・インタプリタ

上述したように、アクティベータ２２８は、ＡＲＦＳＤ・ＶｘＤ３０４内部に実現したバイトコード・インタープリタ３０８上で実行する。アクティベータはＣＡＳ２１０から入手し、ＡＲＦＳＤ・ＶｘＤ３０４によるｂｒｉｑデータ解読に用いるＳＣＤＰクライアントソフトウェアの一部である。アクティベータの形式と内容は図１３を参照にして詳しく説明する。アクティベータは、ＣＡＳ２１０に替わりとなる新しいアクティベータを定期的に要求するようアクティベータに求める保持機能を実現する。よって、タイトル実行を継続するには、ＣＡＳとの通信は維持しなければならない。図示した実施例では、アクティベータ２２８内の保持機構は数値ストリングとして、又は図１３を参照にして説明したように実現してもよい。

【００６１】

アクティベータは、ＡＲＦＳＤ・ＶｘＤ３０４内で実行できる動的バイトコードオブジェクトとして実現される。図７のアクティベータ・ファクトリモジュール７１０を参照して既に説明したように、ＣＡＳは、外部ライブラリ内に常駐させてもよいアクティベータ生成ルーチンを呼び出してアクティベータを生成する

。ＲＡＦＴトークンは上述したようにアクティベータと共にパッケージしてある。アクティベータはいずれタイムアウトし、その後はＳＣＤＰクライアント２１６はＣＡＳを呼び出し、新しいアクティベータを要求しなければならない。アクティベータの寿命はアクティベータのトークン部分に含まれた開始及び終了時間値により決定される。

【００６２】

ＳＣＤＰシステム２００は、アクティベータを用いてＳＣＤＰクライアント２１６へ渡された暗号データを保護する。アクティベータは、ＡＲＦＳＤ・ＶｘＤ３０４内で走ると共にｂｒｉｑの解読を可能にする一片の曖昧化バイトコードとして実現できる。アクティベータがダウンロードされると、更なるＲＰＣをＣＡＳ２１０に対して行い、キーイングデータの送信を完了してもよい。アクティベータ内でのコード曖昧化によりキーの抽出を防ぐことができる。

【００６３】

アクティベータの図示した実現例は、アクティベータ内のキーを守るために遠隔実行を用いる。遠隔実行によりアクティベータは不完全になる。つまり、遠隔実行はアクティベータが連続動作するのに十分な情報を与えるが、アクティベータが新たにコード又はデータを要求する必要がある。ＡＲＦＳＤ・ＶｘＤ３０４内のバイトコード・インタープリタ３０８は、アクティベータから暗号キーデータを抽出するプログラムロジック、コード、又はオブジェクトを包含する。図示した実施例では、アクティベータは図１３を参照して説明したような形式及び内容を備えていればよい。

【００６４】

別の実施例では、アクティベータが曖昧化バイトコードを含むより高度なアクティベータの実現例を用いるが、ＡＲＦＳＤ・ＶｘＤ３０４内のバイトコード・インタープリタ３０８はリッチ命令セットを用いて実現し、曖昧化を単純にできる機会を増やしてもよい。ハードウェアが実現するマイクロプロセッサ命令セットにあった従来の制限が無く、アドレス指定方式及び命令形式用に多くのビットを用いることができる。こうした命令セットの複雑さ及び機密性により、ＳＣＤＰシステム内のコンテンツ引き渡しの安全性を確保する。バイトコードはＶｘＤ

内で走るため、バイトコード・インタープリタ３０８は、他のＶｘＤからエクスポートされたインターフェースを呼び出すかもしれないが、オペレーティングシステムからのＷＩＮ３２機能を呼び出す必要もなく、ＤＬＬを扱う必要もない。

【００６５】

図示した実施例においては、バイトコード・インタープリタ３０８は、ＣＡＳ２１０から受け取ったアクティベータ内のバイトコードを解釈及び実行するのに必要な適切なコード及び／又はプログラムロジックを備えた仮想計算機として実現してある。こうした仮想計算機は、バイトコードを翻訳し、バイトコードストリームからの一時データを全て保存し、バイトコードにより特定される処理を実行するための適切な経路を備えている。バイトコード・インタープリタ３０８を如何に具体的に実現するかは、従って、インタープリタにより実行可能なバイトコードセットに依存する。例えば、バイトコード・インタープリタ３０８は、アクティベータが含むコードの種類に対応するために幾つかの次に挙げたものを含んだ特定の機能を実行可能である。

・ビット式オペレータ　－　暗号化及び配列化ルーチンに有用なけた送り、回転、及び「ビット抽出」機能。

・評価　－　バイトコード・インタープリタにダウンロードした又は変更したバイトコードを解読させ、よってコード及びデータが対応するフラッグ及びデータ保護から分離されるのを防ぐ。

・インターフェース基本命令（言語：primitive）　－　ＳＣＤＰクライアント・バイトコード・インタープリタが、引数配列化およびＣタイプの特定の事前定義データセットの内部化を含む、他のＶｘＤ内の機能を直接呼び出す。ＳＣＤＰクライアント及びＣＡＳは安全ストリームインターフェース基本命令を用いる。例えば、接続データ（特に認証データ）をアクティベータ又は手法が生成されたストリームから抽出するフック。

【００６６】

通常の技能を備えた当業者であれば、バイトコード・インタープリタ３０８は物理的計算機として実現してもよいことは明らかであろう。本明細書に記載した最も単純なアクティベータにおいては、バイトコードはオプションである。よっ

て、バイトコード・インタープリタ３０８もオプションとしてもよい。

【００６７】

通信ライブラリ３１２は、ＡＲＦＳＤ・ＶｘＤモジュール２１８とＲＡＦＴ・ＶｘＤモジュール２２２との間の通信用に用いられる。こうしたライブラリは図３Ｂの通信ライブラリ３０４に類似したもので、ＶｘＤ２１８とＶｘＤ２２０との通信を助ける。

【００６８】

制御モジュール３１０には、インストール抄録を実行し、タイトルを実行し、且つＲＡＦＴトークンを更新するのに必要なアルゴリズムを実行するのに必要なプログラムロジック又はコードが含まれる。更に詳細には、制御モジュール３１０が実行するアルゴリズムは、図４Ａ乃至６及びそれに関する記載箇所に更に詳しく説明してある。

【００６９】

図３Ｄは、ＳＣＤＰクライアント２１６のＲＡＦＴクライアントＶｘＤ２２２を包含する構成要素の概念ブロック図を示す。詳しくは、ＶｘＤ２２２は、ＲＡＦＴ・ＲＰＣライブラリ３１６、キャッシュロジック３１８、及び制御モジュール３２０を包含する。ＲＰＣライブラリ３１６は、本明細書に更に詳しく説明してあるが、ＲＡＦＴプロトコルのクライアント側ＲＰＣレイヤを実現する適切なコード及び／又はオブジェクトを含む。こうしたプログラムロジックは、ＲＡＦＴメッセージの何れかを用いるＲＡＦＴサーバ２０６との通信に使用される。具体的には、モジュール３１６は、図１１を参照して説明するように、ＲＡＦＴパケットヘッダを各ＲＡＦＴプロトコルメッセージに添えるため、且つ適切なＲＡＦＴプロトコルメッセージで応答するために必要なロジックを含む。キャッシュロジック３１８は、ＲＡＦＴプロトコルを用いてＲＡＦＴサーバ２０６から詮索したｂｒｉｑ、又はその一部のキャッシュを行うための適切なコードを含んでいる。モジュール２１８によりキャッシュされたｂｒｉｑの部分は、ＳＣＤＰクライアント２１６が実行しているホストパーソナルコンピュータの一時メモリの一部に保存してもよい。具体的なキャッシュ技法及びそれに関連したロジックは、多数ある周知のキャッシュアルゴリズムに従って実現でき、それは通常の技能を

持った当業者に容易に理解可能である。制御モジュール３２０は、モジュール３１６、３１８に関する上述の機能を管理し且つ図４Ａ乃至６に関連して記載した方法の諸ステップを実行するために必要なプログラムロジック、コード及び／又はオブジェクトを含むように実現される。

【００７０】

タイトル実行

図５Ａ乃至５Ｃのフローチャートは、本発明による典型的なタイトル実行中にＳＣＤＰクライアント２１６により実行される処理ステップを示す。上述したように、ＳＣＤＰクライアントのブラウザ２２４がランチストリングを受け取ると、ランチストリングに関連した多目的インターネットメッセージ拡張仕様（ＭＩＭＥ）タイプがレジストリエントリで探し出され、その結果、ＳＣＤＰクライアント２１６内のランチャモジュール２２０が呼び出される。ステップ６に示したように、呼び出しにが起こると、ランチャ２２０はランチストリングから汎用資源名（ＵＲＮ）を抽出して、ＣＡＳ２１０にＵＲＮからＵＲＬへの変換を要求する。本発明のＵＲＮはｂｒｉｑ内のタイトルの固有識別子である。標準ＵＲＮ形式は以下の通りである。

urn:arepa://vendor/path/titlename[#version]

【００７１】

ＵＲＮにおいては、タイトルへのパスは、ベンダの記憶サーバ内にあるタイトルの現在の位置に正確に一致している必要はない。このパスは分類の便宜を図るものであり、必要ではない。タイトルのバージョン番号はオプションであり、ポンド記号でタイトル名から分離してもよい。ベンダ名は固有性を保証するために中央権威機関に登録してもよい。

【００７２】

汎用資源ロケータ（ＵＲＬ）は、ＲＡＦＴ記憶サーバ内にあるｂｒｉｑの現在の位置を特定する。標準ＵＲＬ形式は以下の通りである。

raft://hostname/path/briqname.brq

【００７３】

ＵＲＬにおいては、パスはＲＡＦＴ記憶サーバ内にあるｂｒｉｑの現在の位置

に正確に一致していなければならない。

【００７４】

図５Ａ乃至５Ｃは、本発明による加入及びタイトル実行中にＳＣＤＰクライアント及び内部モジュールにより実行される処理ステップを示す。図２Ｂの要素も参照すると、ＳＣＤＰクライアントが走るホストコンピュータのユーザは、ウェブブラウザ２２４を用いて、仮想店舗ショーウインドウ２１５から所望のタイトルを選択する。店舗ショーウインドウ２１５はデジタルオッファをウェブブラウザに返すが、ユーザはこのオッファを用いてＥコマースサーバ２０２と購入交渉を行う。Ｅコマースサーバは、未署名のランチストリングをネットワークを介してウェブブラウザに送信する。ランチストリングはＭＩＭＥヘッダでパックされている。ステップ５０２に示したように、ランチストリングがブラウザに受信されると、ランチストリングに付随したＭＩＭＥタイプは、ファイルシステムのレジストリエントリで探し出され、その結果、ＳＣＤＰクライアントのランチャモジュール２２０が呼び出されることになる。処理ステップ５０４に示したように、ランチャモジュール２２０はランチストリングからＵＲＮ値を抽出して、このＵＲＮ値をＣＡＳサーバ２１０に送信する。ランチャ２２０とＣＡＳ２１０との通信は安全なＲＰＣ接続を介して確立される。ＣＡＳ２１０はＵＲＮをＵＲＬに変換し、当該ＵＲＬをＳＣＤＰクライアントに送信する。ＵＲＬが受け取られると、決定ステップ５０６に示したように、ランチャ２２０はＵＲＬヘッダを読み出す要求をＡＲＦＳＤ・ＶｘＤモジュール２１８に渡し、モジュール２１８はその要求をＲＡＦＴクライアントＶｘＤ２２２に渡す。ＶｘＤ２２２は、ＲＡＦＴプロトコルを用いてＲＡＦＴサーバ２０６にその要求を送信する。ＲＡＦＴサーバ２０６は、ＵＲＬを開いてそのヘッダ情報を読み出す。ヘッダ情報はその後、ＲＡＦＴクライアントＶｘＤ２２２へ、そしてＡＲＦＳＤ・ＶｘＤモジュール２１８及びランチャ２２０に戻される。この処理全体は図５Ａの処理ステップ５０８に示されている。次に、処理ステップ５１０に示したように、ランチャモジュール２２０は、ヘッダの内容を用いてホストシステムのアプリケーション検査要求を実行する。

【００７５】

システムの検査要求の完了後に、処理ステップ５１２に示したように、ランチャモジュール２２０は購入許可要求を、安全なＲＰＣ接続を介してＣＡＳ２１０に送信する。購入許可要求に応答して、ＣＡＳ２１０はＲＡＦＴトークンを含んだアクティベータを生成すると、アクティベータは安全なＲＰＣ接続を介してＳＣＤＰクライアント２１６に送信される。決定ステップ５１４に示したようにアクティベータを受け取ると、ステップ５１６に示したように、ランチャモジュール２２０はＲＡＦＴトークン及びアクティベータをインストールする。処理ステップ５１６及び５１８にそれぞれ示したように、アクティベータはＡＲＦＳＤ・ＶｘＤモジュール２１８内にインストールされ、ＶｘＤモジュール２１８は、ＲＡＦＴトークンをＲＡＦＴＶｘＤ内にロードする。処理ステップ５２０に示したように、ＲＡＦＴ・ＶｘＤ２２２は、その後、ＲＡＦＴプロトコルからの適切な命令の何れかを用いてＲＡＦＴトークンをＲＡＦＴサーバ２０６に送信する。次に、処理ステップ５２２に示したように、ＡＲＦＳＤ・ＶｘＤ２１８は、ＶｘＤ２２２との通信を介してＲＡＦＴサーバ２０６にあるｂｒｉｑからスーパーブロックフィールドを読み出し、処理ステップ５２４に示したように、スーパーブロック内のマジックナンバーを検査する。ｂｒｉｑ内のマジックナンバーは、例えば「ＡＲＦＳ」などの固定キャラクタ列（原語：constant sequence of characters）として実現してもよい。

【００７６】

この時点で、処理ステップ５２６に示したように、ランチャモジュール２２０はタイトルの実行可能ファイルを実行し始める。図示した実施例では、実行可能ファイルは、ＲＡＦＴＶｘＤ２２２を介して入手したデータを用いてＡＲＦＳＤ・ＶｘＤ２１８が実現したファイルシステム中に位置したウィンドウズ（Ｒ）実行可能ファイルの形式となっている。

【００７７】

処理ステップ５２８に示したように、ＲＡＦＴ・ＶｘＤ２２２は、ＲＡＦＴサーバ２０６からタイトルディレクトリ及びファイルの検索を開始する。タイトルのディレクトリ及びファイルを包含するデータブロックは、ＲＡＦＴプロトコル及び本明細書に記載されたコマンドを用いてＲＡＦＴサーバ２０６から入手する

。詳しくは、ＶｘＤ２２２は、データブロックをＲＡＦＴサーバ２０６から読み出し開始（言語：read-ahead）方式で入手し、データブロックをキャッシして効率的な解読及び実行を促進する。

【００７８】

処理ステップ５３０に示したように、ＡＲＦＳＤ・ＶｘＤ２１８は、ＣＡＳアクティベータ２１０から検索したアクティベータ、特に解読キーデータを用いてＲＡＦＴサーバ２０６から入手したデータブロックを解読し、且つ保全性検査を行う。上述したように、アクティベータには、ｂｒｉｑ内にあるデータを実行前に解読するのに役立つ暗号か情報が含まれている。処理ステップ５３２に示したように、ＡＲＦＳＤ・ＶｘＤ２１８は、オペレーティングシステムに対してインストール抄録を保持して、タイトル実行に必要なファイルシステムがローカルホスト・パーソナルコンピュータにインストールされているかのような錯覚を作り出す。ＶｘＤ２１８がインストール抄録を保持する処理は、図６を参照して詳しく説明する。

【００７９】

ＣＡＳ２１０から受け取ったＲＡＦＴトークンは、図８を参照して説明してあるように終了時間フィールドを含む。決定ステップ５３４及び処理ステップ５３６に示したように、アクティベータ及びＲＡＦＴトークンが満期つまり無効となる前に、ランチャモジュール２２０は安全なＲＰＣ接続を介して、更新アクティベータ及びＲＡＦＴトークンのペアをＣＡＳサーバ２０６に要求する。処理ステップ５３８に示したように、この新しいアクティベータ及びＲＡＦＴトークンのペアは上述した方法と同様にインストールされ、使用される。

【００８０】

インストール抄録

本発明によれば、タイトルはＳＣＤＰクライアントホストシステム上に「インストール」されることは決してない。ＳＣＤＰクライアントソフトウェアはインストール抄録を作成して、実行中のタイトルがホストコンピュータにインストールされているという錯覚をローカル・オペレーティングシステムに対して維持する。よって、タイトル実行が終了すると、タイトルがホスト・パーソナルコンピ

ュータ上で実行されたことを示す証拠は残らない。タイトルに関連した如何なるファイルもホストシステムのハードディスク上に残らず、例えばタイトルに関連したレジストリ変数などのオペレーティングシステム状態情報も残らない。タイトルが出た後又はシステムクラッシュ後のＳＣＤＰクライアントの状態は、以前と同じである。可能性は低いが唯一の例外は、例えば、他のアプリケーションが行った処理、持続性状態及び保存した文書又はデータなどのユーザがアプリケーションに対して行った変更によるのみである。インストール抄録は、アプリケーションを実行する前に予想されるアプリケーションの状態をロードする方法で達成されるが、これは、アプリケーションが出る際に、持続性パラメータに影響を与えずにこの状態がアンロードされるように行われる。

【００８１】

図１２に関連して説明されているように、本発明による各ｂｒｉｑは１つかそれ以上のタイトルのファイルシステムを含む。以下に説明するように、ｂｒｉｑオーサーは、オーサーユーティリティプログラムを用いて、アプリケーション及びアプリケーション・インストールディレクトリから選択したファイルを抽出する。ｂｒｉｑオーサーは、アプリケーションを正しく実行するのに必要かもしれないレジストリエントリのようなそれ以外の情報も抽出する。オーサープログラムは、選択したファイルと他の情報を組合せ、且つデータベースエントリセット及びｂｒｉｑ形式でファイルシステムを出力として生成する。このｂｒｉｑはＲＡＦＴサーバに記憶される。データベースエントリはＣＡＳサーバに記憶され、キーイング情報及びヘッダチェックサム値などの情報を包含する。

【００８２】

図６は、本発明による、タイトル実行中にインストール抄録を保持するために、ＳＣＤＰクライアント２１６及び内蔵されたモジュール２１８乃至２２０によって実行される処理ステップを示したフローチャートである。ステップ６００に示したように、あるタイトル選択及び購入交渉に続いて、ランチャ２２０及びＡＲＦＳＤ・ＶｘＤ２１８はファイルシステムをマウントし、ステップ６０２に示したように、関連したレジストリエントリをホストシステムのローカルドライブに記憶する。ウィンドウズ（Ｒ）９５、ウィンドウズ（Ｒ）９８、及びウィンド

ウズ（R）NTのファイルマネージャ内の機能及びUNIX（R）オペレーティングシステムの同等の機能は、ファイルディレクトリ及び遠隔位置ファイルの内容を「マウント」し、又はそれらへのコンピュータネットワークを介したアクセスを実現し、データをアクセスする「仮想ドライブ」を生成する。本発明では、ファイルシステムのマウントは、RAFTサーバにSCDPクライアント・オペレーティングシステムインターフェースを介してアクセスするための上述した技法を用いることを包含する。ファイルシステムをマウントすると、タイトルコンテンツ及びそのタイトルに関連したレジストリエントリを含むbriqからデータブロックの全部又は一部はキャッシュすることになり得る。この一連のレジストリエントリはSCDPクライアントのホストシステムメモリにローカル記憶され、タイトルファイルがインストールされたディレクトリなどの情報を含むことができる。ARFSD・VxD218は更に、CASデータベース212から適切なデータベース項目を抽出する。

【0083】

ステップ604に示したように、CASサーバによりSCDPクライアントに送られたアクティベータからのキーイング情報を用いて、briqからのデータブロックは解読され、且つオペレーティングシステム・ファイルシステムとして実行される。タイトル実行中は、データブロックは必要に応じてSCDPクライアントでローカルキャッシュされる。プログラム実行中に、オペレーティングシステムの仮想メモリマネージャ部分内に含まれるようなオペレーティングシステムのデバイスドライバは、ローカル物理ドライブに記憶させたレジストリエントリを要求する。決定ステップ606に示したように、アプリケーションが実行されると、ARFSD・VxD218ははこうした処理要求の解釈を開始する。ステップ608に示したように、該当する場合は、呼び出しは、局所記憶されているレジストリエントリのリストからのエントリで満足される。しかし、後に記載するライトスルー手法を用いてオペレーティングシステムに直接書き込まれる情報もある。

【0084】

決定ステップ610に示したように、アプリケーション実行が終了するまでは

、オペレーティングシステム呼び出しの傍受及び局所記憶されたレジストリエントリを用いたこれら要求の満足は継続される。この時点で、ステップ６１２に示したように、ランチャはＡＲＦＳＤ・ＶｘＤ２１８にファイルシステムをアンマウントつまり切断するよう指示する。その結果、オペレーティングシステム要求は局所記憶されたレジストリエントリに転送されなくなる。局所記憶されたレジストリエントリ及び局所でキャッシュされたデータブロックは消去されるか、上書きしてもよい。その結果、タイトルつまりアプリケーションを実行する前のＳＣＤＰクライアントの状態は、ユーザが意識的に保持しようと願う限られたライトスルーデータを除いてはそのタイトルのインストールの痕跡もなく現状に戻される。

【００８５】

ライトスルー局所記憶

作成者プログラムを用いたオーサーによるｂｒｉｑの生成時に、ファイル及びディレクトリは「ライトスルー」属性のタグを付けることができる。ライトスルーファイル又はディレクトリを内包するｂｒｉｑは、ＬＯＣＬタグ付きのコンテナを内包していることがある。このコンテナは全てのライトスルーディレクトリの完全なパス及び、ＬＤＩＲタグで示される、ライトスルーファイルを内包するあらゆるディレクトリ（ルートディレクトリを除く）のパスを含む。ユーザは局所記憶ファイル用のルートディレクトリのパス名を指定することができる。新しいパス名は、固有性を確保するため、ＵＲＮからのベンダフィールドを含む。この情報は、タイトルのＬＯＣＬコンテナ内のＲＯＯＴタグに記憶される。デフォールトでは、ＡＲＦＳＤ・ＶｘＤは、ローカルドライブに０バイトの空きがあると報告する。ライトスルーファイル又はディレクトリを含まないｂｒｉｑは常に０バイトの空きがあると報告する。タイトルのＬＯＣＬコンテナ内にタグが存在すれば、ＡＲＦＳＤ・ＶｘＤが、局所記憶ディレクトリを内包するドライブ上の空きスペース量を報告するはずであることを示す。タイトルがＬＯＣＬコンテナを必要とするのは、ＲＯＯＴに関してフォールト値以外を指定する必要がある場合のみである。

【００８６】

ライトスルーファイル又はディレクトリを内包したｂｒｉｑ（言い換えれば、ヘッダにＬＯＣＬコンテナを内包したｂｒｉｑ）がロードされると、ＳＣＤＰクライアント内のランチャが局所記憶用のディレクトリをＳＣＤＰインストールディレクトリの下に作成する。このディレクトリは、タイトルのＬＯＣＬコンテナ内でＲＯＯＴタグによって他のディレクトリが指定されていなければ、ＵＲＮから導き出す。ランチャは、ヘッダにＬＤＩＲタグを付けて指定された各ディレクトリ用の局所記憶ディレクトリ内にサブディレクトリを作成する。局所記憶パスのルートパス名及び空きディスクスペースを報告するかどうかをｂｒｉｑロード中にＡＲＦＳＤ・ＶｘＤに渡す。ランチャソフトウェアがアンインストール及びオプションでタイトルが出る時に、局所記憶領域内の全てのファイルは消去される。これらの局所記憶されたファイルはデフォールトでは持続性がある。ランチャは、ｂｒｉｑ内の全てのライトスルーディレクトリ用のディレクトリをローカル記憶装置内に作成する必要がある。

【００８７】

ライトスルーファイルが開始されると、情報は、上述したディレクトリと同様の命名規則を備えた局所記憶領域内のファイルから取り出される。もしそのファイルが局所記憶装置に存在しない場合は、そのファイルはまずｂｒｉｑからコピーされる。ｂｒｉｑ内の元々のファイルは、全ｂｒｉｑ暗号化を別にすれば圧縮や暗号化されていないこともある。ライトスルーファイルを開くと、ローカルディスクのコピーも開かれて、ＡＲＦＳＤ・ＶｘＤファイルハンドルにおける全ての要求は実ファイルハンドルで実行される。

【００８８】

条件付きアクセスサーバ（ＣＡＳ）

図７Ａは、条件付きアクセスサーバ（ＣＡＳ）７００及び付随したデータベース７５０の概念ブロック図である。図示した実施例では、ＣＡＳは、ＰＯＳＩＸ．１（ＩＥＥＥ標準１００３．１，１９９８年）に互換性のあるプラットフォーム上で実行可能なアプリケーション（例えば、カリフォルニア州パロアルト所在のサンマイクロシステムズ社が市販するサンソラリス（Sun Solaris（商標））オペレーティングシステム又は、レッドハットソフトウェア社が市販するリナッ

クスオペレーティングシステム）として実現してもよく、こうしたプラットフォームは図１に示したものと類似のコンピュータアーキテクチャ上で実行できる。ＣＡＳアプリケーション７０２は、データベース・インターフェースモジュール７０４、遠隔手順呼び出しインターフェース７０６、ＵＲＮ－ＵＲＬ変換モジュール７０８、アクティベータファクトリ７１０、及びＵＲＬ検証モジュール７１２を更に包含する。

【００８９】

データベースインターフェースモジュール７０４はＣＡＳデータベース７５０とのインターフェースを取り、市販のデータベース製品を用いて実現してよい。データベース７５０は、更新を要求するトークンのステイデータなどの短期ステイデータ又は、タイトル名、暗号キー情報及びＳＣＤＰシステムを介して入手できるタイトルに関する他の情報などの長期ステイデータを記憶するのに用いることができる。ネットワーク上に複数のＣＡＳサーバが存在していれば、データベース７５０は複数のＣＡＳサーバ７００が共有してもよい。データベースインターフェース７０４及びデータベース７５０は、ＳＱＬ標準データベース問合わせ言語で通信する。ＳＱＬ標準は、米国規格協会（ＡＮＳＩ）が発行している。データベースインターフェース７０４は、サーバ７００により受け取られた問合わせにフィルタをかける一組のオブジェクトを包含する。こうしたフィルタは、データベース問合わせの範囲を狭めカストマイズするのに役立つ。

【００９０】

ＣＡＳサーバ７００はネットワーク２０５を介して残りのＳＣＤＰシステムに接続され、このネットワークは図示した実施例においては、ローカルエリアネットワーク又は広域ネットワークとして実現されたインターネットプロトコルに基づいたネットワークである。サーバ７００は遠隔手順呼び出しモジュール７０６を介してネットワーク２０５とインターフェースをとる。モジュール７０６は、サンマイクロシステムズ社が発行するオープンネットワーク・コンピューティング遠隔手順呼び出し標準（インターネット工学プロジェクトチームが発行したＲＦＣ１０５７）に準拠したコード又はオブジェクトを包含してもよい。こうしたＲＰＣ標準は、ネットワークを介して遠隔通信を試みる２つの実体間のフロー及

び機能呼び出しを制御するコードを定義する。モジュール７０６は、遠隔手順呼び出しをサブルーチン機能呼び出しのように見せる何れかの市販ツールを用いて実現してよい。モジュール７０６を実現するのに有用な製品の一例としては、マサチューセッツ州サウスボロ所在のノーブルネット社が販売するノーブルネット安全ＲＰＣがある。ノーブルネット安全ＲＰＣは、通常のＲＰＣインターフェースに付加的な安全レイヤを提供する。

【００９１】

ＵＲＮ－ＵＲＬ変換モジュール７０８は、ＵＲＮ問合わせをデータベース７５０に受けると対応するＵＲＬを返すコード又は一連のオブジェクトを包含する。こうしたＵＲＮは、ＳＣＤＰクライアントのランチャモジュールからネットワーク２０５を介して受け取られる。ＵＲＮが記憶されるデータベース７５０は複数レコードを備えた順次データベースでよい。モジュール７０８は適切な問合わせをデータベースインターフェース７０４に送り、データベースから適切なＵＲＬを受け取る。モジュール７０８は、その後、ネットワーク上をＲＰＣモジュール７０６を介して対応するＵＲＬをＳＣＤＰクライアントに送信する。或いは、タイトル及び／又はコンテンツサーバの数が限られている環境においては、ＵＲＬはサーバに付随したディスクに記憶してもよく、更に、モジュール７０８は受信したＵＲＮの参照用テーブル変換を実行するプログラムロジックを包含していてもよい。

【００９２】

変換モジュール７０８は、抄録ＵＲＮデータ構造を絶対ＵＲＬデータ構造に変換し、又、一連の変換テーブル及び関連した比較ロジックによって実現してよい。ＵＲＬ検証モジュール７１２は、Ｅコマースサーバ２０２からランチストリング及び、ハッシュコードと暗号化キーによりランチストリングがデジタル署名するタイムスタンプを受信するコード又は同等のオブジェクトを包含する。具体的には、メッセージ認証コードをＣＡＳサーバ７００から受け取ったランチストリングに追加してもよい。このメッセージ認証コードは、ＭＤ５ハッシュアルゴリズムに基づいて生成されたハッシュコードを含んでもよく、更にデータ暗号化規格（ＤＥＳ）を含む複数の暗号化標準に従って生成された暗号化キーを含んでい

てもよい。本明細書で説明したように、デジタル署名されたランチストリングはその後、Ｅコマースサーバ２０２に送られ、更に、クライアントホストシステムのウェブブラウザに返信される。

【００９３】

ＳＣＤＰシステムにおいては、アクティベータは、キーイング情報を安全でない可能性のあるクライアントプロセスに送る機能を果たす。サーバ７００のアクティベータ生成モジュール７１０は、一連のバイトコードを生成すると共に暗号キーをその一連のバイトコードに添えるコード又は適切なオブジェクトを包含する。ある実現化例ではこのキーはデータベース７５０から検索される。アクティベータ生成モジュールの実現様態は、ＳＣＤＰシステム内で用いられるアクティベータの洗練度に部分的に左右される。一連のバイトコード及びそこに付加又は統合されたたキーを包含するアクティベータに関しては、アクティベータ生成モジュール７１０は上述のように実現されている。別の実施例では、キーはアクティベータにもっと安全な方法（例えば、キーをバイトコード列に折り畳む）で統合されており、付加的ロジック及び／又はオブジェクトがモジュール７１０内でそうした機能を実現するのに必要である。例えば、キーを一連のバイトコードに添える替わりに、数を生成したりその他の論理演算を実行するような一定の機能を実行するバイトコード列をアクティベータ内に挿入してもよい。そうした実施例では、モジュール７１０は、複数のバイトコード列から何れかを無作為に選択するロジック又はコード曖昧化技法として本明細書で説明した技法を含んでもよい。こうした実施例では、モジュール７１０は、極めて安全にアクティベータを無作為に生成する能力を備える。或いは、更に高度に洗練されたアクティベータの実現例では、アクティベータモジュール７１０は、外部ライブラリに常駐することもできるアクティベータ生成ルーチンを呼び出してアクティベータを生成できる。

【００９４】

上述したＣＡＳモジュールは、ＳＣＤＰシステム内に５つの主たる機能を含んでいる。第１に、ＣＡＳは、ユーザに暗号化ｂｒｉｑコンテンツの一度だけの使用を許容する暗号アクティベータを提供する。第２に、ＣＡＳにより、ＳＣＤＰ

システムがタイトルの使用を確実且つ的確に追跡し、更に不正使用する目的で設計されたハッキングされたクライアントを開発することが極めて困難な安全モデルを確実にサポートする。第３に、ＣＡＳはＣＡＳ専用キーで署名し且つアクティベータに添付された制限寿命ＲＡＦＴ許可トークンを提供する。ＲＡＦＴクライアントは、許可トークンにＲＡＦＴ要求を含める。ＲＡＦＴサーバはこのトークンを用いて要求されたコンテンツにアクセスする権利がクライアントにあるか検証する。第４に、ＣＡＳはＥコマースサーバソフトウェア・請求書作成システムと対話し、取引を完了する。取引は、購入交渉中には完了せず、エンドユーザがコンテンツを成功裏に実行したことをＣＡＳが確認するまで行われない。第１アクティベータ更新の終了が、タイトルがうまく実行されていることを示す。５番目の機能として、ＣＡＳはタイトル使用報告及びアクティベータ追跡のためのデータベースを維持する。

【００９５】

３種類の経過記録がＣＡＳに関係している。第１に、ＣＡＳの活動は標準ＵＮＩＸ（Ｒ）テキスト経過記録に記録される。この経過記録は診断のためだけに意図されている。第２に、ＣＡＳは、報告及びアクティベータ追跡目的で取引をＣＡＳデータベーステーブルに記録する。これらの記録は、実際の請求書作成目的で用いられるＥコマースサーバシステムによる記録とは別のものである。第３に、ＣＡＳデータベース自身が内部処理経過記録を保持し、その機能は確実にデータベース処理が完了し且つロールバックされるように保証することである。こうした機能はＣＡＳデータベースに内部化してもよい。図示した実施例では、ＣＡＳは、オラクルソフトウェア社から市販されているような市販のデータベースメインテナンスソフトウェアを用い、購入処理が行われたかロールバックされたかを確認する。データベース処理は、上述した金融処理とは異なる。金融処理がデータベース処理であることもあるが、ユーザ名を更新するなどのその他多くの処理がデータベース処理でありえる。

【００９６】

図示した実施例では、ＣＡＳは、システム管理者がＣＡＳの状態（例えば、現在使用されているデータベース接続スレッドの数及びユーザ接続の現在の数、つ

まり、使用されている接続スレッド）を監視できる管理インターフェースをサポートする。更に、ユーザ数及び運転開始以降のデータベース接続の数のピークなどの統計情報や、運転開始以降にユーザ又はデータベース接続が所定限度に達した回数も利用できる。

【００９７】

ＳＣＤＰクライアントはクライアントライブラリを用いてＣＡＳと対話する。クライアントライブラリは各クライアントプラットフォームに固有であってもよいが、その訳は、これはＳＣＤＰクライアントＧＵＩと通信するプラットフォーム固有方法を用いるからである。図示した実施例では、つまりＷＩＮ３２プラットフォームでは、クライアントライブラリはＣＡＳＬＩＢ３２と称する。クライアントライブラリは、ＣＡＳへの移送を示すＣＡＳインターフェースクラスＣＣＡＳと、特定のクライアントセッションを示すＣＣａｓＳｅｓｓｉｏｎとをエクスポートする。アプリケーション・プログラム・インターフェース（ＡＰＩ）により、ＣＡＳＬＩＢ３２クライアントは、複数セッションを通じて複数タイトルに関する交渉を同時に実行できる。ＡＰＩは、ＣＡＳインターフェースを移送プロトコルの細部から隔離する役目を果たす、ＣＡＳとやり取りする情報を示す追加クラスもエキスポートする。こうした方法は、ＣＡｃｔｉｖａｔｏｒ、ＣＵｒｌなどとして実現できる。ＣＣＡＳは、ウィンドウズ（Ｒ）メッセージを送ってクライアントにも非同期的に応答する。

【００９８】

ＣＡＳによるアクティベータサポート

アクティベータの最も単純な実現例は、所与のｂｒｉｑのキーをアクティベータにコンパイルしたバイトコードルーチンである。このアクティベータ実現例では、ＣＡＳは、クライアントを認証し、購入したｂｒｉｑを特定し、アクティベータバイトコードを構築し、更に、アクティベータをダウンロードする。ＳＣＤＰクライアントは、その後、接続を閉じてタイトルを実行する。こうしたアクティベータは前もって生成しておき、ＣＡＳアクティベータファクトリ７１０及びインターフェース７０４によりデータベースから直接検索してもよい。

【００９９】

より高度なアクティベータ実現例では、アクティベータは暗号アルゴリズムを認識し、ＣＡＳからキーを要求する。ＣＡＳは認証情報及び安全データを存在するストリームから受け取っており、必要などんな引数を備えた「要求キー」に対する所定のＲＰＣ応答を用意できる。

【０１００】

別の実現例では、アクティベータは複数段階を必要とする可能性もある新規な機構の任意コードを備えていてもよい。後に説明するように、アクティベータは、不透明引き数を備え且つ「テクニック」の指定付きの遠隔手順呼び出しをＣＡＳに発してもよい。その後、ＣＡＳは、この不透明データをこのテクニックに送り、テクニックはオペックデータをクライアントに返すか、他の呼び出し又はその他のサービスに呼び出しを行う。ＣＡＳ自信がインタプリタを備えていれば、ＣＡＳはアクティベータ及びテクニックのコードをデータベースから検索できる。全てのアクティベータが予め生成されていれば、いずれのテクニックに関しても多くのアクティベータが存在し得る。或いは、曖昧化及び多くの曖昧化具体例を如何に組み合わせるかに関する規則集のデータベースをＣＡＳに管理させてもよい。

【０１０１】

ＣＡＳは、所与のクライアント、製品、購入品に適したアクティベータを選択する。ＣＡＳは、そのアクティベータを届け、付加的ＲＰＣを介してそのアクティベータを「サポート」する。例えば所与のｂｒｉｑに対する単純な「要求キー」などの多くのＣＡＳ・ＲＰＣを予め定義できる。こうしたＲＰＣは選択したアクティベータに基づいて制限できる。例えば、殆どのクライアントは、単純な「要求キー」呼び出しを許可されないが、アクティベータによる使用をテクニックが予期する如何なる呼び出しでも実行することが必要となる。

【０１０２】

図７Ｂを参照すると、加入及びタイトル実行処理中にＣＡＳサーバ７００が実行する処理ステップが示されている。具体的には、ＣＡＳサーバ７００は、図９及びそれに関連した記載で説明されているように、ランチストリングを受け取るが、ステップ７２０に示したように、送信元はＥコマースサーバである。次に、

ステップ７２２に示したように、ＣＡＳはランチストリングに署名する。ＣＡＳは、専用暗号キーでこのランチストリングに「署名」する。処理ステップ７２４に示したように、署名済みのランチストリングは、その後ＣＡＳサーバ７００から、広帯域ネットワークに接続されたホストシステムで実行されているＳＣＤＰクライアントに送られる。図５Ａ乃至５Ｃに関連して説明したように、ＳＣＤＰクライアントはランチストリングからＵＲＮを抽出し、このＵＲＮをＣＡＳ７００に送信する。ステップ７２６に示したように、ＣＡＳ７００はこのＵＲＮをＳＣＤＰクライアントから受け取り、処理ステップ７２８に示したように、ＵＲＮからＵＲＬへの変換を行う。上述したように、ＣＡＳ７００は、モジュール７０８を用いてこのＵＲＮ－ＵＲＬ変換を行う。こうした変換はデータベース７５０へ問合わせたり、テーブル参照アルゴリズムを使用することもあるが、それはモジュール７０８の実現方法による。処理ステップ７２８に示したように、ＣＡＳ７００は、ＵＲＬリストをＳＣＤＰクライアントに送信する。次に、処理ステップ７３０に示したように、ＣＡＳ７００は、ＳＣＤＰクライアントから許可要求を受け取る。ＳＣＤＰクライアントからのこの購入許可要求はランチストリングを含む。その後、処理ステップ７３２に示したように、ＣＡＳ７００は、ランチストリングを検証して、このランチストリングが以前に自分が署名したものか、複数条件付きアクセスサーバを含む実現例であれば、別の権限付与されたサーバが署名したものかを判断する。本明細書で説明したように、ＣＡＳサーバのモジュール７１０の実現方法に従ってアクティベータは生成される。

【０１０３】

処理ステップ７３６に示したように、次に、ＣＡＳ７００は、ＲＡＦＴトークンとアクティベータをＳＣＤＰクライアントに送信する。ＣＡＳ７００は、データベース７５０からＲＡＦＴトークンを検索する。このＲＡＦＴトークンは、本明細書で説明し、図８に示した形式を備えている。本明細書で説明したように、アクティベータ及びＲＡＦＴトークンにより、ＳＣＤＰクライアントは所望のタイトルにアクセスし、タイトルデータの実行を開始できる。この段階で、決定ステップ７３８に示したように、アクティベータトークン更新要求がＳＣＤＰクライアントから送られるまでは、このＳＣＤＰクライアントに関しては何の動作も

行わない。処理ステップ７４０に示したように、ＳＣＤＰクライアントから最初の更新要求を受け取ると、ＣＡＳ７００は、タイトル購入をＥコマースサーバに通知する。この取引のＥコマースサーバへの通知には、ユーザがこの特定タイトルの代金を支払ったことを示す実際の応答記録が含まれる。タイトルがＳＣＤＰクライアント上で正しく実行されていることを示す第１更新要求が出されるまで、こうした通知はなされない。ＣＡＳからＳＣＤＰクライアントに当初送られたアクティベータ内のタイムアウト機構は、所定の期間後に無効つまり満了となり、タイトルが適切に実行されいることを表す。ＣＡＳは、処理ステップ７４２に示したように、新しいトークンを発行し、要求しているＳＣＤＰクライアントにこのペアを送信する。ＲＡＦＴトークンの寿命は、ＲＡＦＴトークンの開始時間及び停止時間フィールドに示してあるように、アクティベータと共にＳＣＤＰクライアントに最初に送信されたトークンの寿命より長くてもよい。ＳＣＤＰクライアントからのその後のアクティベータ／トークン更新要求があっても、ＣＡＳがＥコマースサーバにタイトル購入を通知することはない。上述したように、ＳＣＤＰクライアントとＣＡＳとの間の全ての通信は、安全なＲＰＣ接続を介するので、こうした接続はＲＰＣ標準に準拠する市販の製品を用いて確立させてよい。

【０１０４】

通常の技能を備えた当業者なら理解するだろうが、図７Ｄで概観した処理は、ＳＣＤＰクライアントとの、タイトル実行終了と共に終わる関係においてＣＡＳが実行する諸ステップに注目したものである。ＣＡＳは、幾つかの異なるスレッドが図示した処理の様々なステップを同時実行するマルチタスク・アプリケーションとして実現できることは、通常の技能を備えた当業者には明白であろう。従って、ＣＡＳは特定のＳＣＤＰクライアントの要求を満たす一方、同時に他のＳＣＤＰクライアントからの要求にも対応可能である。

【０１０５】

ＲＰＣ移送

ＣＡＳとＣＡＳＬＩＢ３２は、ノーブルネット安全ＲＰＣなどの標準に基づいた遠隔手順呼び出しライブラリを介して通信する。ＳＣＤＰクライアントはＣＡ

Ｓに複数の呼び出しを同期で行い、ＣＡＳはこれら呼び出しを処理のためスレッドに割り当てる。ＣＡＳＬＩＢ３２は非同期的インターフェースを接続されたＧＵＩに提供し、それはこれらの同期ＲＰＣ要求をキューに入れ且つ背景スレッドから取り出す。高い処理能力を提供するため、ＣＡＳは、タスク実行のために用いることができるスレッドを準備してプールしておく。このスレッドプールは再使用可能なＣ＋＋クラスである。入ってくるタスクはＲＰＣレイヤで捕捉され、スレッドプールのキューに入れ、最終的には組み入れ処理でなくスレッドで処理される。スレッドプールによって、ＣＡＳは、より効率よく同時処理を行うことができ、短いロードスパイク下で動作を向上させる。ＲＰＣ呼び出しはタグ付けした後に解放できるスレッド安全メモリを割り付ける必要があるが、その理由は、ＲＰＣ移送がそれらを送信し終わるまではバッファは解放できないからである。ＣＡＳは、スレッドＩＤによりメモリを消去できる再使用可能Ｃ＋＋メモリプールクラスを用いる。

【０１０６】

ＣＡＳは、ウェブサーバのようなステートレス（原語：stateless）サーバとして実現してもよい。ステートレスサーバは、より多くのサーバ計算機を配置し且つ入ってくる接続を、これらサーバに分配する「総当たり式」ソフトウェアを用いて容易に拡大できるという利点がある。これは、ＳＣＤＰクライアントの後の要求が、それが元々接続したサーバの所に行く必要がないからである。ＣＡＳは、要求間に接続ソケットＴＣＰストリームを維持し、移送セッションキーなどの情報が取り付けられるようにする。この接続が切られると、ＣＡＳＬＩＢ３２は別のＣＡＳ処理にも再接続を試みるので、状態をＣＡＳＬＩＢ３２に又はデータベースの中にプッシュするのが好ましい。

【０１０７】

処理量を増やすために、ＣＡＳは、活動状態にある複数データベース接続のプールを用いるように設計されている。サーバスレッドはプールから接続を要求し、データベースの接続待ち時間を最小化するため、必要に応じて背景で不動作接続を再接続する。データベース接続プールは再使用可能Ｃ＋＋クラスとして実現されている。ＣＡＳは、ＤＢＯｊｅｃｔと呼ばれる抄録データベース・インター

フェースを用いるが、このインターフェースは再使用可能Ｃ＋＋クラスとして実現されており、ＣＡＳの他のデータベースへの移植を容易にする。

【０１０８】

ＲＡＦＴトークン

ＳＣＤＰシステムの安全モデルを全般的に向上させるため、ＣＡＳは、ＳＣＤＰクライアントに署名済みＲＡＦＴ許可トークンを与える。このＲＡＦＴトークンは、特定のＳＣＤＰクライアントが特定のＵＲＮに所定の時間アクセスするのを許可する。ＣＡＳは、標準化された公開かぎデジタル署名アルゴリズムを用いてＲＡＦＴトークンにデジタル署名する。ＲＡＦＴサーバの実行可能なコンテンツにアクセスするためには、ＲＡＦＴ・ＶｘＤはそのトークンをそのサーバに渡さなければならない。ＲＡＦＴサーバは、ＣＡＳのデジタル署名を検証し、その後、トークンのコンテンツを検証する。ＲＡＦＴトークン８００は、ＣＡＳの管理ドメイン内の如何なる数のＲＡＦＴサーバに対しても有効で、言い換えれば、広帯域サービスプロバイダは自己のネットワーク上に複数サーバをインストールでき、ＲＡＦＴトークンはそれらの何れにも受け入れられることとなる。

【０１０９】

図示した実施例では、ＲＡＦＴトークンは、図８に示した形式を備えたデータ構成で実現されている。ＲＡＦＴトークン８００は、ＵＲＮ、ＵＲＮ長８０４、開始時間８０６、終了時間８０８、ＩＰアドレス８１０、及びＣＡＳ署名８１２を包含する。ＵＲＮ８０２及び付随した長さ８０４は、ＲＡＦＴトークンがアンロックする特定のタイトルを定義する。開始時間８０６及び終了時間８０８はトークンの寿命を定義する。このＵＲＮの形式は既に説明した。ＲＡＦＴ許可トークンは、ＲＡＦＴクライアントのＩＰアドレスをネットワークのバイト順に３２ビット値として含む。このトークンは更に、要求されたＵＲＮ及び３２ビット開始及び終了時間も含む。こうした時間は、ＰＯＳＩＸ１００３．１－１９８８に「新時代の始めからの秒数」又は概ね１９７０年１月１日、グリニッジ平均時００：００：００からの秒数として定義されている。ＲＡＦＴサーバが真正確認できるように、ＣＡＳはＣＡＳグループの専用キーでトークンに署名する。ＲＡＦＴサーバは、サーバの現在時間がトークンの時間帯に入っていなければ、アクセ

スを拒否する。ＩＰアドレスはアクティベータ／トークンを要求するＳＣＤＰクライアントのネットワークアドレスを定義する。トークンを提出したＳＣＤＰクライアントが同じＩＰアドレスを持っていなければ、ＲＡＦＴサーバはアクセスを拒否することで、他のクライアントが不正入手したトークンの使用を防止する。

【０１１０】

ＲＡＦＴトークンはアクティベータの一部としてクライアントに送信される。ＲＡＦＴトークンはアクティベータと共に更新される。アクティベータは寿命制限メカニズムに基づき構成されている。ＳＣＤＰクライアントは、ＲＰＣ機構を介してＣＡＳ要求を出し、現在のアクティベータが無効つまり満期になる前にアクティベータとトークンのペアを更新する。

【０１１１】

ランダムアクセスファイル移送プロトコル及びサーバ

図１０は、ＲＡＦＴサーバ１０００及び付随したデータベース１０５０のブロック図を概念的に示す。図示した実施例では、ＲＡＦＴサーバ１０００はＰＯＳＩＸ．１（米国電気電子学会標準１００３．１，１９８８）と互換性のあるプラットフォーム上で実行可能なアプリケーションとして（例えば、カリフォルニア州パロアルト所在のサンマイクロシステムズ社が市販するサンソラリス（Sun Solaris（商標））オペレーティングシステム又は、レッドハットソフトウェア社が市販するリナックスオペレーティングシステム）として実現してもよく、こうしたプラットフォームは図１に示したものと類似のコンピュータアーキテクチャ上で実行できる。

【０１１２】

ＲＡＦＴサーバはＲＡＦＴアプリケーション１００２及びオペレーティングシステム上で実行されるシンプルネットワーク管理プロトコル（ＳＮＭＰ）マスターエージェント１００４として実現できる。ＳＮＭＰマスターエージェント１００４を実現するのに適して市販品は、ＳＮＭＰリサーチインク社から入手できるエマネートがある。マスターエージェント１００４はＳＮＭＰ標準に従った公開済みのアプリケーションプログラムを用いてネットワーク２０５と通信する。

【０１１３】

ＲＡＦＴアプリケーション１００２は、ＰＯＳＩＸ（ポータブル・オペレーティングシステム・インターフェース標準）ファイル出入力モジュール１００６、ファイルシステムインターフェース１００８、ＳＮＭＰ計装モジュール１０１０（つまりＲＡＦＴ・ＳＮＭＰサブエージェント）及びネットワーク／ＲＰＣ／ＲＡＦＴプロトコル・インターフェースモジュール１０１２を包含する。

【０１１４】

ＳＮＭＰ計装モジュール１０１０は、システム管理者がネットワークの帯域幅を抑えてネットワーク性能を向上させるのに有用な統計的及びロジスティック情報を収集するオブジェクト又は対応するコードを内包している。モジュール１０１０は、ＲＡＦＴサーバ１０００のオプションの装置である。

【０１１５】

ＲＰＣ・ＲＡＦＴプロトコル１０１２は、本明細書に記載されたように所有権を主張できるＲＰＣプロトコルを用いてＩＰに基づいたネットワーク２０５とのインターフェースをとる。モジュール１０１２は、このプロトコルを実現し且つＲＡＦＴトークンの内容を検証するのに必要なコート及び／又はオブジェクトを含んでいる。

【０１１６】

ファイル入出力モジュール１００６は、米国電気電子学会（ＩＥＥＥ）が発行しているＰＯＳＩＸ標準１００３．１に従ったオブジェクト指向で実現してもよい。ＰＯＳＩＸ・Ｉ／Ｏモジュール１００６は、メモリディスク１０５０にローカル・ファイルシステム・インターフェース抄録を提供する。図１０に概念的に示したメモリ１０５０は、ｂｒｉｑの形式で複数タイトルを記憶するのに用いられる。本実施例では、解読したｂｒｉｑのヘッダ部分と符号化されているｂｒｉｑの本体部分は、一緒に記憶される。しかし、これら部分には、モジュール１００６及び１００８を用いてお互いに独立してアクセスする。ファイルシステム・インターフェース１００８は、特定のｂｒｉｑに対する要求を受け且つｂｒｉｑが記憶されるメモリ１０５０中のディレクトリ及びファイル中にｂｒｉｑをマップするプログラムロジックを含んでいる。こうした方法で、ファイルシステムイ

ンターフェース１００８はＳＣＤＰシステムからのネットワーク要求とメモリ１０５０との間のインターフェースとして機能する。図示した実施例においては、メモリ１０５０は、ＲＡＩＤディスクアレイ又はディスクファームなどの一つ以上のディスクとして実現してもよい。ファイルシステム・インターフェース１００８は、ファイル入出力モジュール１００６とネットワーク・プロトコルモジュール１０１２との間のインターフェースとして機能し、且つ、本明細書で説明してあるように、ファイル及びｂｒｉｑにアクセスするためのプログラムロジックを実現する。

【０１１７】

ＳＮＭＰマスターエージェント１００４は、ＲＡＦＴアプリケーションに埋め込まれているＲＡＦＴ・ＳＮＭＰサブエージェントに代わってＳＮＭＰプロトコルサービスを提供する。ＲＡＦＴアプリケーションはＳＮＭＰサブエージェントを使って、その管理を遠隔ＳＮＭＰマネージャにアクセス可能にする。

【０１１８】

次の幾つかのステップは、ＳＣＤＰクライアントとＲＡＦＴサーバとの相互作用を説明するものであり、ランチャがタイトルをランチする。ランチャはＣＡＳサーバに連絡して、要求されたＵＲＮに対応するＵＲＬのリストを入手する。ＵＲＬは、特定のｂｒｉｑの位置（このｂｒｉｑが存在するＲＡＦＴサーバも含む）を割り出す。各ＲＡＦＴ・ＵＲＬに関して、最も適切なＵＲＬ選択の助けとなるよう、重みを返すようにしてもよい。ＵＲＬの重み値は高ければ、高いほど好ましい。

【０１１９】

ＣＡＳによるＵＲＮ－ＵＲＬ変換に続いて、ＳＣＤＰクライアントはＣＡＳに、ＣＡＳ交換に関する説明で述べたように購入要求を送る。購入要求に応答して、ＣＡＳサーバは、ＳＣＤＰクライアントに、選択したＵＲＮのＲＡＦＴ許可トークンを含んだアクティベータを与える。許可トークンは選択したＵＲＮに関連した複数ＵＲＬの何れにも有効である。

【０１２０】

その後、ランチャはＵＲＬのリストを検査して、ＲＡＦＴ・ＵＲＬが存在する

か判断する。もしＲＡＦＴ・ＵＲＬが存在すれば、ランチャはＲＡＦＴ・ＵＲＬのリストのみをＲＡＦＴアクセストークンと共にＡＲＦＳＤ・ＶｘＤに送り、ＡＲＦＳＤ・ＶｘＤはこの情報をＲＡＦＴクライアント、つまりＳＣＤＰクライアントのＲＡＦＴ・ＶｘＤに送る。ランチャはＲＡＦＴ・ＵＲＬのそれぞれの重み付けもする。これらの重みはＵＲＮ－ＵＲＬ変換においてＣＡＳが付けたものとは異なってもよい。ＲＡＦＴクライアントは、その後、ＵＲＬリストに指定されたＲＡＦＴサーバの何れかと接続を確立する。ＲＡＦＴクライアントは、ＵＲＬに付けた重みを用いてどのＲＡＦＴサーバに最初に連絡するかを決定するための適切なプログラムロジックをこのクライアント自身に含んでいてもよい。

【０１２１】

その後、ＲＡＦＴクライアントは、ＲＡＦＴサーバ１０００上のｂｒｉｑを開こうとする。このクライアントはプロトコルバージョン、パス名（ＵＲＬからの）、及びＲＡＦＴアクセストークンを特定する。プロトコルバージョンは、ＲＡＦＴクライアント及びＲＡＦＴサーバがプロトコルに関して互換性があるかを確認するのに用いる３２ビット値である。アクセスの正当性を確認するため、ＲＡＦＴサーバは、トークン内のＵＲＮがｂｒｉｑヘッダ内のリストにあるものかを確認する。ＲＡＦＴサーバ１０００は、開ける際にＲＡＦＴトークンの開始及び終了時間をチェックする。もしＲＡＦＴ＿ＯＰＥＮが成功すると、ＲＡＦＴサーバは、ＲＡＦＴファイルハンドル及び、ｂｒｉｑタグのハッシュのようなキャッシュ処理に用いられるｂｒｉｑの固有ＩＤを返す。

【０１２２】

ＲＡＦＴサーバが満期時間を確認するために、ＲＡＦＴサーバの時間は所定間隔までＣＡＳと同期される。したがって、ＲＡＦＴサーバは現在の時間より早い開始時間は許容し、その間隔の終了まではアクセスを拒否しない。トークン満期時間は、アクティベータ保持時間に、変動するネットワーク及びサーバ待ち時間を加えたものを提唱する。

【０１２３】

その後のＲＡＦＴ読みだし要求が出されると、そうした各要求のたびに、ＲＡＦＴサーバはアクセストークンが満期になっていないかを確認する。ＲＡＦＴサ

ーバは、該当するクライアントの有効なアクセストークンがなければ、要求を無視する。

【０１２４】

ＲＡＦＴアクセストークンはいずれ満期となる。ＳＣＤＰクライアントのアクティベータ保持機能が、現在のトークンが満期となる前に新しいＲＡＦＴトークンを入手する責任を負っている。これにより、ＲＡＦＴトークンが確実にタイミング良く更新され、アクセス失敗は通常の動作条件下では起こらない。ＲＡＦＴクライアントがＲＡＦＴ＿ＯＰＥＮの間にトークンをＲＡＦＴサーバに送ると、ＲＡＦＴクライアントは開始時間から満期時間までのトークンの有効期間を計算しなければならない。ＲＡＦＴクライアントはＣＡＳの公開かぎなしではトークンの内容の正当性を確認できないので、ＲＡＦＴクライアントは、このトークンが有効かどうかを確認するのに、更新時間を設定する前にＲＡＦＴ＿ＯＰＥＮが成功するのを待つ必要がある。しかし、更新時間は、ＲＡＦＴクライアントがトークンを受け取った時間に基づいており、ＲＡＦＴ＿ＯＰＥＮ完了時間に基づいてはいない。サーバへの接続を確実に継続するには、ＲＡＦＴクライアントは、トークン満期時間に先だってＣＡＳから新規ＲＡＦＴアクセストークンを要求する。新しいＲＡＦＴアクセストークンを受け取ると、ＲＡＦＴクライアントは、あたらに入手したトークンと共にＲＡＦＴ＿ＲＥＦＲＥＳＨ処理をＲＡＦＴサーバに送付する。

【０１２５】

ＲＡＦＴクライアントがｂｒｉｑへのアクセスを完了すると、ＲＡＦＴクライアントはＲＡＦＴファイルハンドルでＲＡＦＴ＿ＣＬＯＳＥメッセージを送る。もしＲＡＦＴサーバとＲＡＦＴクライアントのと接続が切断されていれば、ＲＡＦＴサーバはその接続に対応する全ての開いているファイルを自動的に閉じる。

【０１２６】

ＲＡＦＴパケットヘッダ定義

ＲＡＦＴプロトコルに従った全ての通信には、図１１に示したようにＲＡＦＴパケットヘッダ１１００が含まれている。ＲＡＦＴパケットヘッダ１１００は、手順番号データフィールド１１０２、シーケンス番号データフィールド１１０４

、パケット長フィールド１１０６及び状態データフィールド１１０８を包含するデータ構造体として実現できる。手順番号データフィールド１１０２はＲＡＦＴプロトコルメッセージタイプを特定し、整数形式で実現できる。シーケンス番号フィールド１１０４は要求に対して応答を一致させるのに用いられ、整数形式で実現できる。シーケンス番号は、一つの接続に関してのみ固有性がある。パケット長フィールド１１０６は、ヘッダのサイズを含まないパケットデータのサイズを示し、整数形式で実現できる。状態フィールド１１０８はＲＡＦＴ要求から状態を示し、整数形式で実現できる。非ゼロ状態は、要求が失敗したことを示す。異なるプロトコルメッセージに対して異なる状態コードが返される。しかし、ゼロ状態は要求が完全に成功したことを示す。非ゼロ状態の場合はパケット長フィールドがゼロに設定され、これは要求が失敗した場合はパケットデータが返されないことを示す。ＲＡＦＴプロトコルに従って、パケットヘッダにはＲＡＦＴパケットデータが続く。

【０１２７】

ＲＡＦＴプロトコルメッセージ

ＲＡＦＴプロトコルは、ｂｒｉｑアクセス及びＲＡＦＴトークン管理を可能にする４つの異なるプロトコルメッセージからなる。ＴＰＣ接続を確立すると、要求者のプロトコルバージョンを特定するために、最初のＲＡＦＴプロトコルメッセージには、その引き数の一つとしてこのプロトコルバージョンが含まれている。ＲＡＦＴプロトコルメッセージのリスト及び記述は以下の通りである。ＲＡＦＴ＿ＯＰＥＮ機能は、プロトコルバージョン、トークン長、ＲＡＦＴアクセストークン、パス長、及びＮＵＬで終わる全パス名で呼び出される。成功すると、ＲＡＦＴファイルハンドル、ＲＡＦＴ・ＩＤ、及びＲＡＦＴサーバがサポートする最大読み出し長となる。ＲＡＦＴ・ＩＤを用いてＳＣＤＰクライアントキャッシュ・タグを生成できる。失敗が起こった場合に備え、ＲＡＦＴ・ＩＤは、複数ＲＡＦＴサーバにおける一貫したキャッシュを達成するためのｂｒｉｑ・ＩＤでよい。最大読み出し長は、ＲＡＦＴクライアントにＲＡＦＴ＿ＲＥＡＤ処理中に要求できるデータ量を知らせるのが目的である。

【０１２８】

ＲＡＦＴ＿ＲＥＦＲＥＳＨ＿ＴＯＫＥＮ機能により、ＲＡＦＴクライアントは新しいＲＡＦＴアクセストークンを使ってＲＡＦＴサーバを更新できる。この機能はトークン長、ＲＡＦＴアクセストークン、及びＲＡＦＴファイルハンドルで呼び出される。成功すると、新しいＲＡＦＴアクセストークンは指定されたハンドルに関連した現在のトークンと入れ替わり、トークンの満期時間を長くする。新しいトークンが有効でなければ、現在のトークンは保持される。この機能はデータを返さないが、ヘッダ内の状態は成功又は失敗を反映するように更新される。

【０１２９】

ＲＡＦＴ＿ＲＥＡＤ機能は、ＲＡＦＴ＿ＯＰＥＮ呼び出しから戻されたＲＡＦＴファイルハンドル、６４ビット・オフセット及び長さで呼び出される。要求したデータにアクセスするには、ＲＡＦＴファイルハンドルは、有効なアクセストークンに関連付けられていなければならない。

【０１３０】

ＲＡＦＴ＿ＣＬＯＳＥ機能は、開いているＲＡＦＴファイルハンドルを閉じるのに用いる。この呼び出しはＲＡＦＴファイルハンドルを取り、データは返さない。しかし、ヘッダの状態は成功又は失敗を反映するように更新される。

【０１３１】

ランチストリング

図９は、本発明によるランチストリング９００を示す。図９に示すようにランチストリング９００は、ＵＲＮデータフィールド９０２、店舗ＩＤデータフィールド９０４、商品タイプデータフィールド９０６、加入ドメインデータフィールド９０８、及び金額データフィールド９１０を包含するデータ構造体として実現できる。ＵＲＮ９０２は所望のコンテンツを固有に識別し、更に、本明細書に記載したように実現できる。店舗ＩＤデータフィールド９０４は特定の店舗ショーウインドウをＥコマースシステムに特定し、且つ、数字列、英数字列、又は整数形式で実現してよい。店舗ＩＤは、報告のために異なる店舗ショーウインドウからの取引を分離するために使われる。複数店舗が本当に同じ組織に属していれば、単一の店舗ＩＤを共有してもよい。商品タイプ９０６は、取引が加入による購

入かミクロ取引による購入かを示し、且つ、数字列、英数字列、又は整数形式で実現してよい。加入処理は、一回の支払いで特定期間はタイトル又は一組の複数タイトルを無制限に利用するためのものである。ミクロ取引はユーザの借方勘定への請求金額であり、「一回の利用に対する支払い」モデルをサポートするのに用いられる。加入ドメイン９０８は、当該取引が「今週のホットなゲームパック」や「個人事業用のアプリケーションパッケージ」などの特定の加入オッファーを購入する際の対象となっているかを示す。加入ドメインは数字列、英数字列、又は整数形式で実現してよい。金額フィールド９１０は、ミクロ取引の購入額を示し、整数形式で実現してよい。

【０１３２】

図１４に示したように、ランチストリング９００の内容は、Ｅコマースサーバ・フロントエンドモジュール１４０８によって生成される。ＣＡＳは、例えば標準化された公開かぎデジタル署名アルゴリズムを用いてランチストリング９００にデジタル署名する。その後は、ランチストリング９００はＣＡＳグループの専用キーを特定する付加的ＣＡＳ署名フィールド９１２を包含する。ランチストリングは、ＳＣＤＰクライアントにＥコマースシステムを介してサービス業務の一環として送る。ＳＣＤＰクライアントは、上述のようにＣＡＳとのランチ前の交渉中に、ランチストリングをＣＡＳに送り返す。

【０１３３】

Ｅコマースシステム

本発明と共に用いるのに適した電子通商ソフトウェアアプリケーション（以下Ｅコマースシステムと称する）は、マサチューセッツ州ケンブリッジ所在のオープンマーケット社から市販されているトランスアクト４．０である。Ｅコマースソフトウェアは、ユーザ勘定を管理し、金融取引を実行するために用いられており、例えば、１）ユーザ勘定情報を管理し、２）購入及び支払いを管理し、３）クレジットカード情報を収集及び検証し、４）取引を完了するために用いられる。

【０１３４】

図２を再度参照すると、Ｅコマースサーバ２０２は、図１を参照して説明した

ものと類似のコンピュータアーキテクチャ上を走るサーバアプリケーションを包含する。このアプリケーションは、サン社のソラリスなどのオペレーティングシステム又はサーバタイプのアプリケーションを実行するよう設計されたその他のオペレーティングシステム上で動作するよう設計されている。図１４を参照すると、Ｅコマースサーバ１４は、オペレーティングシステム１４０４が走るハードウェアプラットホーム１４０２を包含する。実際のＥコマースサーバアプリケーション１４０６は、フロントエンドモジュール１４０８及びバックエンドモジュール１４１０をＳＣＤＰシステム２００のその他の様々な構成要素に提示する。具体的には、サーバ１４００のフロントエンドモジュール１４０８は、ウェブサーバ・フロントエンドをＳＣＤＰシステム２００に対してネットワーク２０５を介して提示するように実現できる。こうしたフロントエンドは、現在インターネット上に存在する他のウェブサーバと似たものである。サーバ１４００のバックエンド４１０は、請求書作成データベース２０４とのインターフェースを取り、データベースの問合わせと、交渉及びタイトルの購入に関連した取引及びミクロ取引の実行とに必要なロジック及び／又はオブジェクトを実現する。上述のように、Ｅコマースサーバ１４００は、専用ＬＡＮ又はインターネットなどの広域ネットワークを介して、銀行やクレジットカード調査及び電子貸方記入などのサービスを行う第三者信用貸し処理サーバに接続できる。サーバ１４００のフロントエンドモジュール１４０４及びバックエンドモジュール１４１０は、共通ゲートウェイインターフェース（ＣＧＩ）規格に従って書かれた一連のスクリプトを介して通信する。通常の技能を備えた当業者にとっては、他の市販のＥコマースサーバアプリケーションをここに述べたもの以外にＳＣＤＰシステムと共に使用可能であることは明白であろう。

【０１３５】

データベース２０４はサーバ２０２に付随しており、従来のシリアルデータベースを包含してもよく、取引を進めるのに必要な信用貸し及び請求書作成情報を記憶するのに用いられる。

【０１３６】

サーバ１４００のフロントエンドモジュール１４０８は、図９を参照して更に

詳しく説明したようにランチストリングを生成するのにコード又はオブジェクトを更に包含する。一旦生成されると、ランチストリングはデジタル署名のためにＣＡＳサーバに送られる。

【０１３７】

図示した実施例では、Ｅコマースシステムはサーバ及び店舗ショーウインドウを包含し、この両者が協力して、ユーザがカタログ内を移動できるようにし、購入情報を受付且つ承認する。Ｅコマースシステムは、外部構成要素と対話するのにオープンウェブに基ずくアーキテクチャを用いる。本発明のＳＣＤＰシステムソフトウェアモジュールは、ＵＲＬをＥコマースソフトウェアのウェブサーバフロントエンドに通知することで、Ｅコマースソフトウェアと通信する。この通知に応答して、トランスアクトはＵＲＬで符号化された特定の引き数でＣＧＩプログラムを呼び出す。ＣＧＩ呼び出しを介してＵＲＬを評価すると、トランスアクトソフトウェアがデータベースの状態を変更する。処理シーケンス全体は、単に一組のＵＲＬを評価することで終了する。Ｅコマースシステムは、ユーザ勘定又はクレジットカード情報などのクライアントデータを捕捉し且つ保持する。

【０１３８】

Ｅコマースシステムが、店舗ショーウインドウに商取引能力を与え且つウェブを介したクレジットカード取引を実行する能力を備えた機能を完備したシステムであれば、ＣＡＳとＥコマースシステムとの対話は主に３つの異なる場所で行われる。ユーザがタイトルを購入すると、ユーザは、サービス業務ＵＲＬと呼ばれるリンクをその上に含んだ「デジタル領収書」と称するページを受け取る。このサービス業務ＵＲＬは、実際は、ＣＡＳからランチストリングを入手するのが目的のＣＧＩプログラムである。後に更に詳しく述べるように、ランチストリングは、ＣＡＳが後にユーザのソフトウェアに対する権利を確認する共にＥコマースシステムと処理を終了するために必要な全情報の集まりである。この情報はＣＡＳのみが理解できる形式で返され、ＣＡＳは後にそれ自身のランチストリングを検査する。ランチストリングをクライアントのブラウザに返すと、ブラウザがＳＣＤＰクライアント内部でランチャを起動し且つランチストリングをランチャに回す。後に、ランチャはランチストリングをＣＡＳに送って、アクティベータを

要求できる。ＣＡＳはランチストリングを検査して、もし当該購入が決定していれば、成功するかを確認することをＥコマースサーバに要求する。しかし、ＣＡＳはまだこの取引を成立させない。この時点で、ＣＡＳはアクティベータをランチャに返して、タイトル実行が開始される。最初のアクティベータの寿命は短く設定されている。例えば、最初のアクティベータが満期になる直前に、ＳＣＤＰクライアントＶｘＤがランチャに通知して、ＣＡＳにアクティベータを更新するよう要求する。アクティベータの第１回目の更新が実行されると、ＣＡＳＬＩＢ３２が再度ランチストリングを提供し、今回はＣＡＳはＥコマースサーバとの間で取引を完了する。取引の完了を延期することで、請求書作成の前にタイトルがＳＣＤＰクライアント計算機で正しく実行されていることをＳＣＤＰシステムが間違いなく確認できる。

【０１３９】

ＳＣＤＰシステムは５つの異なる購入モデルをサポートする。最初の購入モデルの「タイトル加入」では、所定の時間は特定タイトルへの無制限のアクセスができる。「アーケードゲームパック」などのパッケージ加入である第２購入モデルは、限られた時間内に一組の複数タイトルに無制限のアクセスを提供する。こうしたパッケージ加入に含まれるタイトルセットは時間が経つと変わることもある。例えば、ユーザが「ホットな新しいゲームパック」への加入を購入したとすると、このパッケージで利用できるタイトルは当初の加入購入から一週間から二週間経つと変わることもある。「１回の使用毎の支払い」の第３購入モデルは、時間無制限で一度だけのアクセスを提供する。「時間に基づく請求」の第４番目の購入モデルでは、ユーザはタイトル実行時間に応じて料金を請求されるか、特定の時間ブロックを購入できる。「月払い」の第５番目の購入モデルでは、ＳＣＤＰシステムは既存のマルチサーバオペレーション（ＭＳＯ）又は電話会社の請求システムに組み込まれ、料金を顧客の月々の請求書に加算する。細かな変更点を含んだこれ以外の購入モデルを加えることもできる。

【０１４０】

仮想店舗ショーウインドウ

仮想店舗ショーウインドウサーバ２１５及び付随のデータベース２１３は、Ｓ

ＣＤＰシステム２００のクライアント及び将来のクライアントに仮想カタログを提示する。図示した実施例では、サーバ２１５は、例えばサーバハードウェア上で実行されるオペレーティングシステム上で実行されるサーバアプリケーションなどの従来のウェブサーバとして実現でき、Ｅコマースサーバ２０２に関連して説明したものと類似のものでよい。店舗ショーウインドウアプリケーションは、一連の品揃えをクライアントが通常のネットワークブラウザで検索できるように表示するグラフィック・ユーザインターフェースを含む。こうした品揃えは特定タイトル名、タイトルの簡単な説明、要する費用又は購入の選択肢を含み、映画やオーディオクリップなどのマルチメディアタイトルの場合は、タイトルコンテンツの短いサンプルなどを含んでいてもよい。更に、各タイトル選択対象には対応するＵＲＮが付随している。店舗ショーウインドウは、データベース２１３と対話する適切なデータベース問合わせエンジンを実現する。尚、データベース２１３には、タイトル、説明、料金、デジタルオッファー、及びＵＲＮ情報をＳＣＤＰシステム２００内の大量のタイトルに関して記憶することができる。特定タイトルが選択されるとそれに応答して、店舗ショーウインドウアプリケーションのロジックが該当するＵＲＮに関してデータベース２１３に問合わせを行い、本明細書に記載した方法で適切な情報をＥコマースサーバ２０２に送る。

【０１４１】

図示した実施例では、上述したように、仮想店舗ショーウインドウサーバ２１５及びデータベース２１３は、専用の安全なローカルエリアネットワーク２０５を介してキャッシュサーバ２１０に接続されている。しかし、ＳＣＤＰシステム２００は、ローカルエリアネットワークを介するのでなく、例えばインターネットなどの広域ネットワークを介してキャッシュサーバ２１０及びＥコマースサーバ２０２に当業者に理解できる方法で接続された１つ以上の仮想店舗ショーウインドウを用いて実現できることは、通常の技能を備えた当業者には明らかであろう。こうした実現例は店舗ショーウインドウサーバは公共ネットワーク上に位置するが、様々な情報の部分集合が将来のクライアントの目に触れる可能性がある。例えば、加入料金を支払うクライアントは、タイトル及び関連する購入選択肢に関して最低の情報しか提供しないかもしれない公共ネットワーク上の店舗ショ

ーウインドウサーバにアクセスする一般大衆よりも、大量の情報及び／又はタイトルデータのサンプルを提供する専用ネットワーク上の店舗ショーウインドウサーバにアクセスするかもしれない。

【０１４２】

ｂｒｉｑ形式

図１２は、本発明によるｂｒｉｑ及びその構成要素のブロック図を概念的に示す。図示したように、ｂｒｉｑ１２００は、ｂｒｉｑヘッダ１２０２、暗号ブロック１２０４、スーパーブロック１２０６、及び１つかそれ以上のタイトル１２０８Ａ乃至１２０８Ｎを包含する。ｂｒｉｑヘッダ１２０２は、システム登録情報、解像度、アプリケーションタイトル、及びＵＲＬなどの、ＳＣＤＰクライアント内のランチャモジュールが使う情報を含む。暗号ブロック１２０４は、タイトルが符合化されているか、そしてもしそうならその符号化に用いられた暗号キーバージョンを特定するためにＳＣＤＰクライアント内のＡＲＦＳＤ・ＶｘＤが用いる。スーパーブロック１２０６は、ｂｒｉｑサイズ、作成データ、ルートディレクトリが存在するエントリなどのｂｒｉｑに関する一般的な情報を含むことが可能である。タイトル１２０８Ａ乃至１２０８Ｎは、それぞれ１つのディレクトリ及び特定のタイトルに関連した１つ又はそれ以上のファイルを含むことができる。本明細書で説明したように、ｂｒｉｑはＲＡＦＴサーバに記憶し、ＲＡＦＴプロトコルを用いてＳＣＤＰクライアントによって遠隔アクセスされ、ローカルファイルシステムとしてホストのオペレーティングシステムに提示される。

【０１４３】

本発明によれば、一つ又はそれ以上のタイトルが、図１２を参照して説明したように、ｂｒｉｑ形式で処理及びパッケージ化される。タイトルをｂｒｉｑ形式にする処理は以下の通りである。第１に、ウィンドウズ（Ｒ）のオペレーティングシステム内のビューアユーティティのようなユーティティツールを用いて、タイトルからレジストリ情報を抽出する。こうしたレジストリエントリは、ファイル名、ディレクトリ名、及びコンフィギュレーション引用などの特定タイトルを実行するのに必要な最小限の情報セットを包含できる。抽出したレジストリエントリはファイルに入れられる。次に、これらレジストリエントリを含んだファイ

ルを作成者プログラムに提供する。本実施例では、作成者プログラムは、タイトル及びレジストリエントリを包含するデータを取って、こうした情報を現在利用可能な多くの暗号化アルゴリズムの何れかに従って暗号化する機能がある。結果として生成される暗号化ファイルは、図１２のディレクトリ１２０８Ａ乃至１２０８Ｎに示したように、従来のディレクトリ階層に記憶される。次に、このファイルシステムのルートディレクトリ及びこのファイルシステムのサイズなどを含んだ付加的メタ情報は、図１２に示したようにｂｒｉｑ１２００のスーパーブロック１２０６に記憶される。次に、ｂｒｉｑ内の暗号化情報を解読するのに必要な暗号キーに関する情報は、暗号ブロック１２０４に記憶される。暗号ブロック１２０４内の情報は、キーバージョン及び使用された暗号タイプの記述を特定するデータを包含できる。ｂｒｉｑ・ＵＲＬ及びシステム要件などの情報は、実行可能ファイル及びタイトルの名前、ネットワークドライブ及び付加的タグのマップと共にｂｒｉｑヘッダ１２０２に入れられる。図１２に示したように、ｂｒｉｑヘッダ１２０２に含まれる情報は暗号化されない。

【０１４４】

アクティベータ

アクティベータは図１３に示したような形式を備える。具体的には、アクティベータ１３００は、トークン１３０２、許可データ１３０４、暗号キー１３０６、及びオプションで１つかそれ以上のバイトコード１３０８乃至１３１２を包含する。図示した実施例では、トークン１３０２は、図８に関連して説明したＲＡＦＴトークン８００に類似のものでよい。許可データ１３０４は、ＣＡＳサーバから新しいアクティベータを要求する際にＳＣＤＰクライアントが使用する「保持」データを包含する。こうした許可データは、単純な数値列又はコードで実現してもよいし、更に、クライアントに前もって関連づけられたデータのハッシュのようなより洗練された高度な実現例でもよい。キー３０６は、ｂｒｉｑ内に含まれたデータを、実行前に解読するのに有用な暗号データを包含する。暗号データを含む解読キー３０６は、ｂｒｉｑデータ解読に役立つ、バイトコードインタプリタ３０８が抽出し且つＲＡＦＴ・ＶｘＤに送られるビット列を包含できる。

【０１４５】

単純な実施例では、アクティベータ１３００は、トークン１３０２、許可データ１３０４、及びキー１３０６のみを包含する。より高度な実施例では、１つ又はそれ以上のバイトコード１３０８乃至１３１２が含まれる。図示した実施例においては、バイトコードは実質的に、バイトコードインタプリタ３０８として実現されている物理又は仮想計算機の何れかで実行可能な命令群である。図示した実施例においては、バイトコードインタープリタ３０８は、アクティベータから送られたこうしたバイトコードを実行する能力のある仮想計算機を包含する。アクティベータ１３００で使用可能なバイトコード１乃至Ｎの種類及び性質は後に説明する。バイトコードインタープリタ３０８は図３Ｃを参照して説明してある。

【０１４６】

コード曖昧化

プログラムの核心部はフロー及び基本命令に分解できる。通常は、フローは、基本命令からより高いレベルの抄録を構築することも含む。最適化には、冗長基本命令を結合すること、フローを配列し直して類似の構造体を結合して除去すること、及びパターンを認識してそれらをより効率的なパターンと交換することが含まれる。最適化により、元々の仕様書の指定に従ってプログラムの動作が維持される。曖昧化処理により１つ以上の正しい結果が得られることもある。無作為に選択するのでなく、正しいバリアントの全体又は部分集合を並列に生成すれば、個別生成にはコスト高になるが全体的にはより効率的になる。

【０１４７】

一般的には、最適化には、問題に対する解決策を見つけ、よりよい解決策を得るためにそうした解決策を改良することが含まれる。実際のコンパイルに当たっては、高レベルコードの単純に生成された正しい表現式を、その正確性を維持しつつより効率的なコードに変換することを意味する。最悪化もこの正確性を保持できるが、曖昧化形式の逆コンパイルが困難なので効率が犠牲になる。

【０１４８】

フロントエンドとアセンブラステージを分離することで、異なるレベルにおいて最悪化子（原語：pessimizer）を挿入でき、且つ最悪化において高度の柔軟性

を提供する例えばＬｉｓｐ／Ｓｃｈｅｍｅのような他の高級言語を後から使用できる。多くの最悪化手法を本発明で使用できるが、それには、１）バイトコードストリームをローカル再整理し且つ曖昧化するアセンブラレベルピープホール最悪化子、２）一定の構造的最悪化に対しより自然なインターフェースを提供する、高級言語とアセンブラとの間の翻訳レイヤを曝す中級言語最悪化子、３）高級言語コードに総称（原語：generic)処理を実際に行う代わりに、ある機能を表現する複数の方法をコーダに指定させ、その後、コーダがコンパイラに既に開始された選択肢の組合せ論的拡張を備えた形式を直接生成させるような、高級マニュアル最悪化子が含まれる。

【０１４９】

理論的には、誰かがアクティベータをシングルステップして、アクティベータの行う変更を監視して、ｂｒｉｑの解読法を発見したり、更に単純には、ｂｒｉｑが解読されたら停止して、メモリからクリアテキストをダンプすることも可能ではある。翻訳困難な「曖昧化」手法で書かれた、異なるバイトコードシーケンスを用い、且つ合い鍵のような同一物を再使用する事を避けることで、本発明は人間の逆コンパイラの作業を困難にし、自動解析を不可能にする。バイトコードにより、権限を持たないクラッカーの１度のダウンロードに対する作業を任意により時間の掛かるものとし、それが他のダウンロードには利用できないようになる。

【０１５０】

本発明のアクティベータに有用な曖昧化手法の例には次のようなものがある。

・処理毎に大量のアルゴリズムの中から選択して、同一オブジェクトに対する２回目の要求にもコードが大きく異なるようにする。

・例えばコンパイラ最適化手法を用いて、動作維持処理をバイトコードに直接適用する。

・ＳＣＤＰクライアントに複数のバイトコードセットをサポートさせるか、バイトコードリスト自身を暗号キーさせる。

・自己修飾バイトコード。

・「トラップドア」バイトコードストリーム（例えばバイトコードシーケンスを

生成する）及び部分集合を拾い出してバイトコード主体を有用なアルゴリズムにマップするマップ関数。制約条件を定義して、その後、役立つシーケンスをスペース中で探す必要があるかもしれない。
・存在するコードにパターンによって関連する可能性のある、注意を逸らすものとしての「デッドコード」バイトコード。
・一定のバイトコードを使用しない。例えば、コードは後続の実行では意味が異なる。（高級ツールは作業アルゴリズムに割り込んでこれらを生成できる。この延長上には、特定の位置又はレジスタを参照する如何なる命令も使用しないことが含まれる。）
・暗号具体例で用いられる「単項」演算子。
・バイトコードのパラメータ（例えば、使用頻度、非相関要素など）に基づいてそのコードのマッピングを最適化する。
・暗号をバイトコードに直接具体化する際に、部分キー／スケジュールまたはコードシーケンスを引き渡して、「標準」形式のキーでないキーを生成する。
・後のコールバックで追加バイトコードをバイトコードにダウンロードさせるか、サーバにバイトコード変更を非同期的に送信させる。
・現在の環境データを、バイトコード、データ、キーイングデータ、ｂｒｉｑそのもののような弱いエントロピー又はその環境内のその他の２進数、又はダウンロードしたバイトコードのソースとして使用する。

【０１５１】

実際に曖昧化したものは、それらがどのように互いに組み合わされるのか、又はどうやってそれらを処理するのかについての情報を与えるフレームワーク内に生成され得るのが理想的である。

【０１５２】

テクニック（技法／手法）

アクティベータの強度を上げるもう一つの方法は、アクティベータを不完全にして、アクティベータがＣＡＳと追加連絡しなければ動作を継続できないようにすればよい。「テクニック」とは、ＣＡＳ内部で実行し且つ要求をサポートするためにカストマイズした一片のコードである。複数のテクニックを用いてもよい

が、単一のテクニックである種類に属する複数アクティベータには十分である。単純なテクニックは、ＣＡＳ内部にハードコード化して実現したり、動的にロードされたバイトコード又は共有オブジェクトで実現できる。テクニックプロトコルにするアクティベータは、ＳＣＤＰクライアントからの移送用の存在するＲＰＣ上のレイヤとし、テクニックが定義済みメッセージを備える手間を省くことができる。本発明では、アクティベータバイトコード及びテクニックバイトコードは別の言語として扱うことができる。テクニックコードは、暗号ルーチン全体用の単一バイトコードを単に備えていればよい。

【０１５３】

本発明のアクティベータ内に曖昧化バイトコードを実現するためには、次の構成要素を用いる。１）バイトコードインタープリタ、２）バイトコードアセンブラ、３）暗号バイトコードルーチン、４）有益な地点でアクティベータにコールインするＡＲＦＳ・ＶｘＤへのインターフェース、５）アクティベータがＣＡＳ内の具体化されたテクニックと通信できるようにする、本明細書で述べたプロトコル、６）ＣＡＳアクティベータ製造機能（アクティベータファクトリ７１０）。

【０１５４】

本明細書に説明されたシステムは、専用イントラネットだけでなく広帯域ネットワーク上でもコンテンツのオンデマンドでの安全な引き渡しを容易にすることが分かるであろう。

【０１５５】

こうして説明した本発明は、ソフトウェアのみ、ハードウェアのみ、又は専用ハードウェアをサポートするためにファームウェアの形式で記憶されたプログラムコードを含んだハードウェアとソフトウェアとの組合せで実現してもよい。上述の実施例の一つのソフトウェア実現例は、図１のディスケット１４２、ＣＤ－ＲＯＭ１４７、ＲＯＭ１１５、又は固定ディス１５２などのコンピュータ読出し可能媒体のような有形媒体に固定された一連のコンピュータ命令又は、モデム又は他のインターフェース機器（例えば、媒体１９１を介してネットワーク１９５に接続された通信アダプタ１９０）を介して搬送波でコンピュータシステムに通

信可能な一連のコンピュータ命令を包含できる。媒体１９１は、光通信又はアナログ通信回線を含むがそれには限定されない有形媒体でもよいし、マイクロ波、赤外線、又はその他の通信手法を含むがそれには限定されないワイヤレス技法を用いて実現してもよい。これらの一連のコンピュータ命令は有形媒体に含まれていても搬送波に乗っていても、本発明に関連して既に説明した機能の全て又は一部を具現化するものである。通常の技能を備えた当業者であれば、こうしたコンピュータ命令はコンピュータアーキテクチャ又はオペレーティングシステムで用いられる多くのプログラミング言語で書くことができ、又、機械実行可能な形式で存在可能であることが理解できるであろう。更に、こうした命令は、半導体、磁気、光学、その他のメモリデバイスを含むがそれに限定されない、現在又は将来のメモリ技術を用いて記憶させてもよいし、マイクロ波、赤外線、又はその他の通信手法を含むがそれには限定されない現在又は将来の通信技術を用いて送信してもよい。こうしたコンピュータプログラムは、印刷文書又は電子文書（例えば、システムＲＯＭ又は固定ディスク上にコンピュータシステムを予めロードした収縮包装したソフトウェア、又は、インターネット又はWWWなどのネットワークを上でサーバ又は電子掲示板を介して販売する）を付けて取り外し可能媒体として販売することも考慮されている。

【０１５６】

本発明の様々な例示的実施例を開示してきたが、通常の技能を備えた当業者には、本発明の精神及び範囲から逸脱することなく本発明の利点の一部を提供できる様々な変更及び修正が可能であることは理解できるであろう。通常の技能を備えた当業者には、同一の機能を持った他の構成要素を適切に用いることが可能なことは明白であろう。更に、本発明の方法は、適切なプロセッサ命令を用いて全てソフトウェアから具体化することもできるし、ハードウェアロジック及びソフトウェアロジックを組み合わせて用いたハイブリッドとしても具体化して、同様の効果を得ることができる。

【０１５７】

以下に特許請求の範囲を記載する。

【図面の簡単な説明】

本発明の上記並びに他の特徴、目的及び利点は、添付図面と併せて下記の詳細な説明を参照することで更に良く理解されるであろう。

【図１】

本発明で使用するのに適するコンピュータシステムのブロック図である。

【図２】

（Ａ）本発明のコンテンツの安全な引き渡しシステムを実行することができる広帯域ネットワークの概念ブロック図である。

（Ｂ）本発明のシステムの要素及び本発明による、他のネットワークの要素との相互作用を示している概念ブロック図である。

【図３】

（Ａ）本発明によるＳＣＤＰの概念ブロック図である。

（Ｂ）図３ＡのＳＣＤＰクライアントのランチャモジュールの概念ブロック図である。

（Ｃ）図３ＡのＳＣＤＰクライアントのＡＲＦＳ・ＶｘＤモジュールの概念ブロック図である。

（Ｄ）図３ＤのＳＣＤＰクライアントのＲＡＦＴ・ＶｘＤモジュールの概念ブロック図である。

【図４】

（Ａ）乃至（Ｂ）本発明による、コンテンツへの加入手順及びタイトルのランチ手順を示すフローチャートを合わせて示す。

【図５】

（Ａ）乃至（Ｃ）本発明による、ＳＣＤＰクライアントによって実行される手順を段階的に示すフローチャートを合わせて示す。

【図６】

本発明による、ＳＣＤＰクライアント構成要素によって実行される手順を示すフローチャートである。

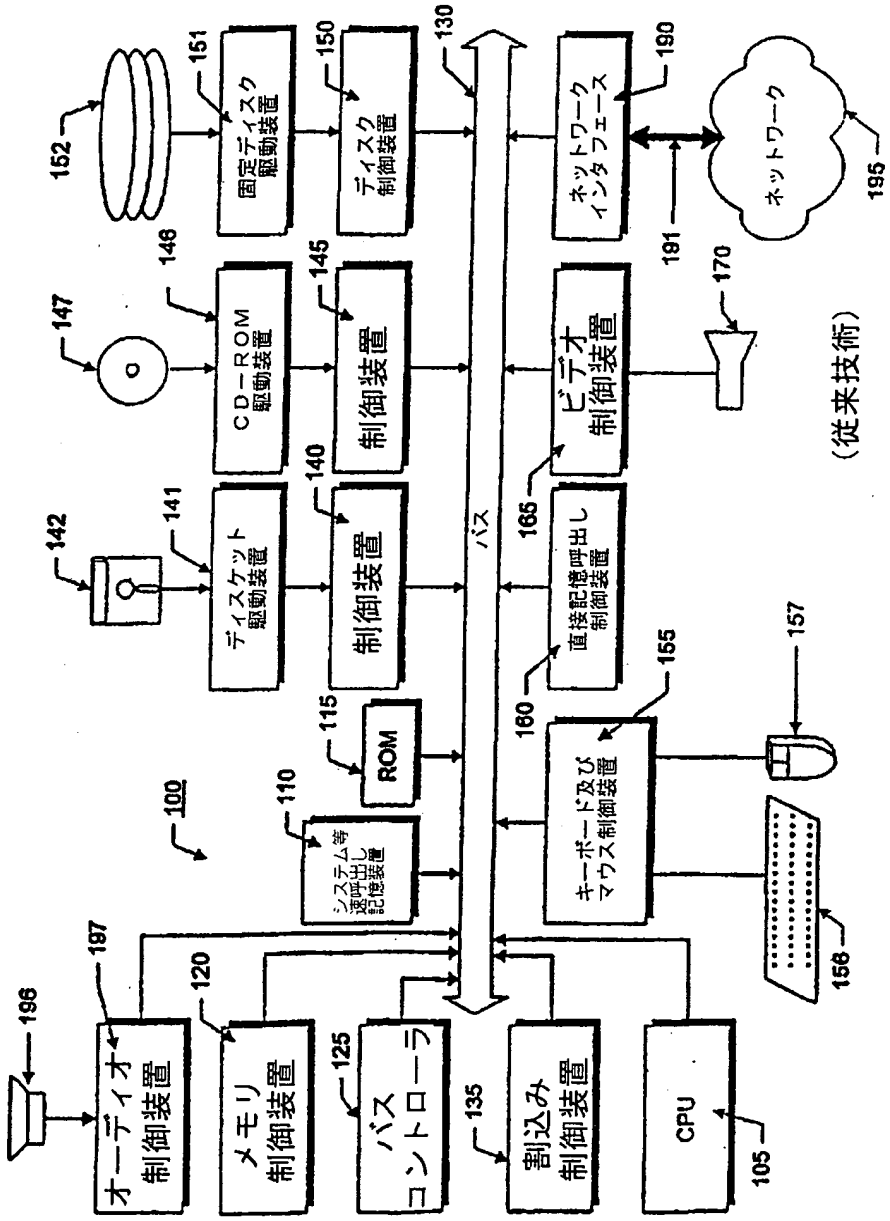
【図７】

（Ａ）本発明による図２のＣＡＳサーバの概念図である。

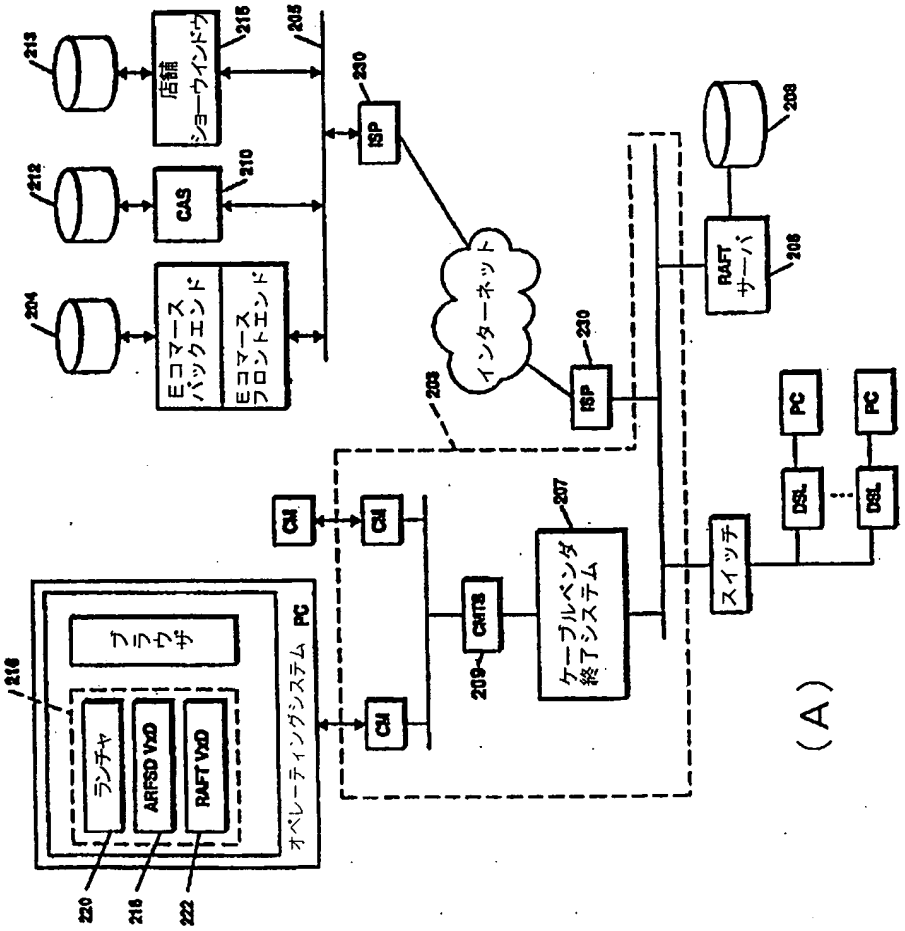
（Ｂ）本発明による、ＣＡＳサーバによって実行される手順を示すフローチャ

ートである。
【図８】
本発明によるＲＡＦＴトークンの概念図である。
【図９】
本発明によるランチストリングの概念図である。
【図１０】
本発明による図２のＲＡＦＴサーバの概念図である。
【図１１】
本発明によるＲＡＦＴパケットヘッダの概念図である。
【図１２】
本発明によるｂｒｉｑデータパッケージの概念ブロック図である。
【図１３】
本発明によるアクティベータの概念ブロック図である。
【図１４】
図１４は、本発明によるＥコマースの概念ブロック図である。

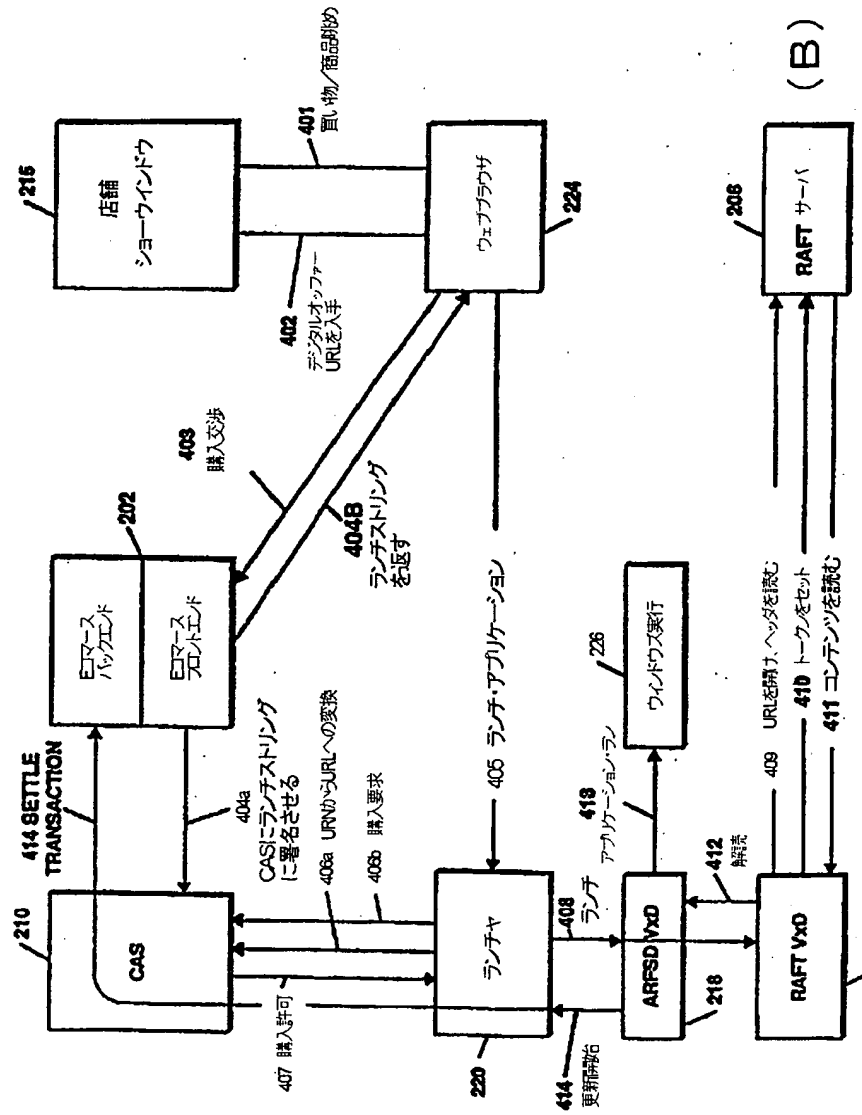
【図１】


100
105
CPU
110
システム等
遠呼出し
記憶装置
115
ROM
120
メモリ
制御装置
125
バス
コントローラ
130
バス
135
割込み
制御装置
140
制御装置
141
ディスケット
駆動装置
142
145
制御装置
146
CD－ROM
駆動装置
147
150
ディスク
制御装置
151
固定ディスク
駆動装置
152
155
キーボード及び
マウス制御装置
157
158
160
直接記憶呼出し
制御装置
165
ビデオ
制御装置
170
190
ネットワーク
インタフェース
191
195
ネットワーク
196
197
オーディオ
制御装置
（従来技術）

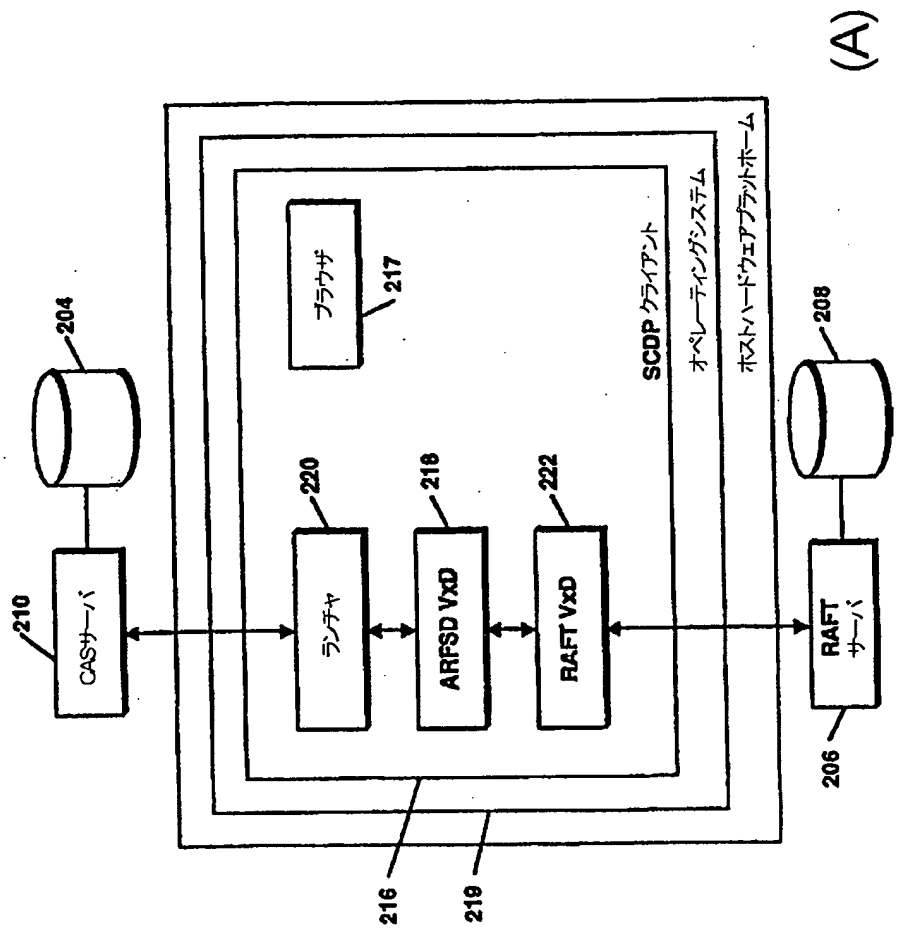
【図２Ａ】


店舗ショーウインドウ
CAS
Eコマースバックエンド
Eコマースフロントエンド
ISP
インターネット
RAFTサーバ
PC
DSL
スイッチ
ケーブルベンダ終了システム
CMTS
CM
ブラウザ
ランチャ
ARFSD VxD
RAFT VxD
オペレーティングシステム
（A）

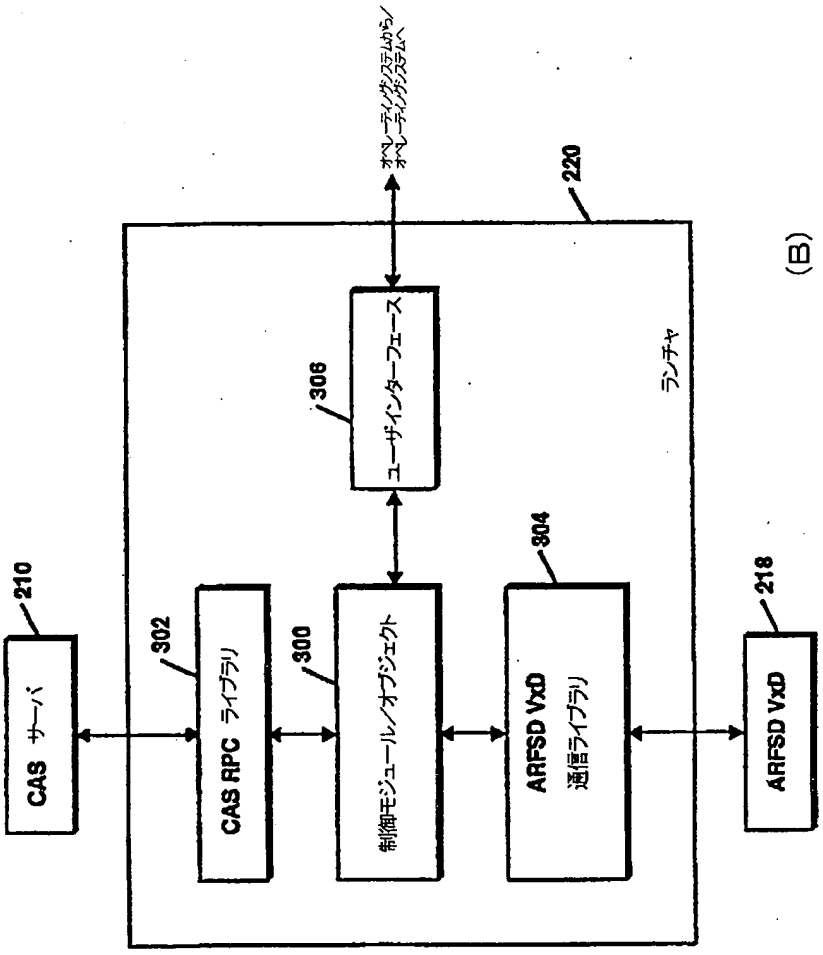
【図２Ｂ】


店舗
ショーウインドウ
216
401 買い物／商品紹介
402 デジタルオッファー URLを入手
ウェブブラウザ
224
RAFT サーバ
208
403 購入交渉
404B ランチストリング を返す
202
EDマース バックエンド
EDマース フロントエンド
405 ランチ・アプリケーション
226
ウィンドウズ実行
CAS
210
414 SETTLE TRANSACTION
404a CASにランチストリング に署名させる
406a URNからURLへの変換
406b 購入要求
407 購入許可
ランチャ
220
408 ランチ
418 アプリケーション・ラン
ARFSD VxD
218
412 解読
409 URLを読み、ヘッダを読む
410 トークをセット
411 コンテンツを読む
RAFT VxD
222
414 更新開始
（B）

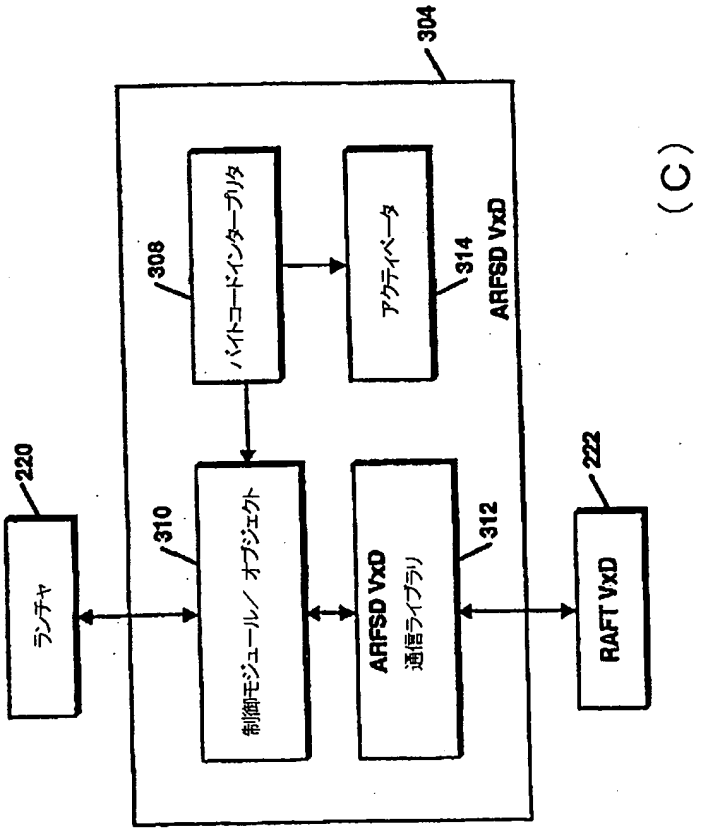
【図３Ａ】


(A)
ホストハードウェアプラットホーム
オペレーティングシステム
SCDP クライアント
ブラウザ
217
204
208
220
218
222
ランチャ
ARFSD VxD
RAFT VxD
210
CASサーバ
RAFT
サーバ
206
216
219

【図３Ｂ】

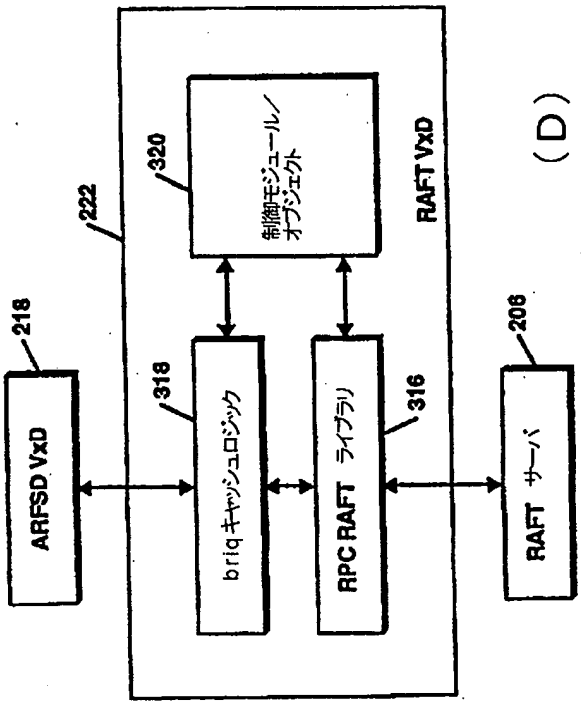

オペレーティングシステムから/
オペレーティングシステムへ
220
ユーザインターフェース
306
ランチャ
(B)
210
CAS サーバ
302
CAS RPC ライブラリ
300
制御モジュール/オブジェクト
304
ARFSD VxD
通信ライブラリ
218
ARFSD VxD

【図３Ｃ】

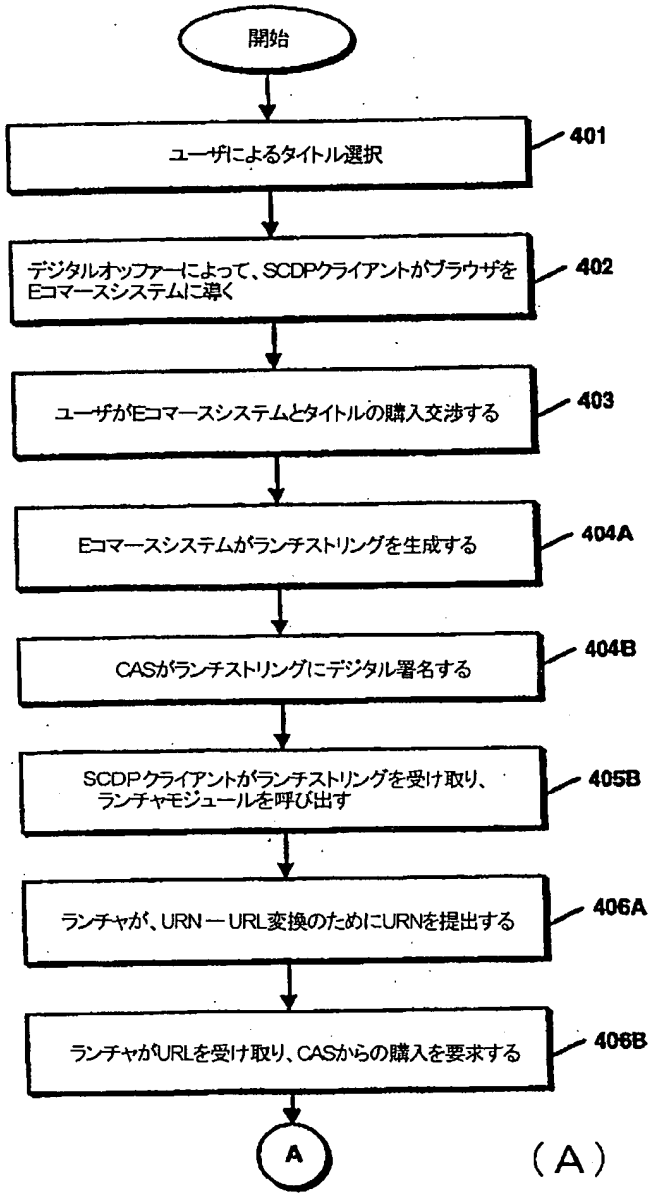

304
308
バイトコードインタープリタ
アクティベータ
314
ARIFSD VxD
220
310
制御モジュール／オブジェクト
ARIFSD VxD
通信ライブラリ
312
222
RAFT VxD
ランチャ

（Ｃ）

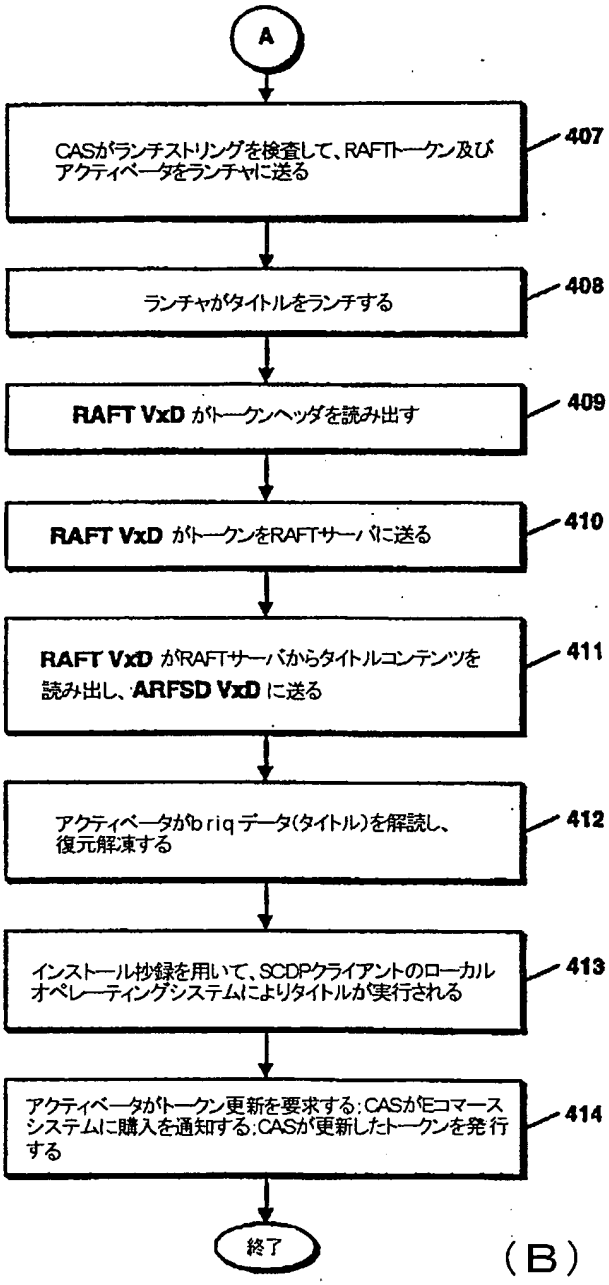
【図３Ｄ】


218
ARFSD VxD
222
318
briqキャッシュロジック
320
制御モジュール／オブジェクト
316
RPC RAFT ライブラリ
RAFT VxD
206
RAFT サーバ
（D）

【図４Ａ】

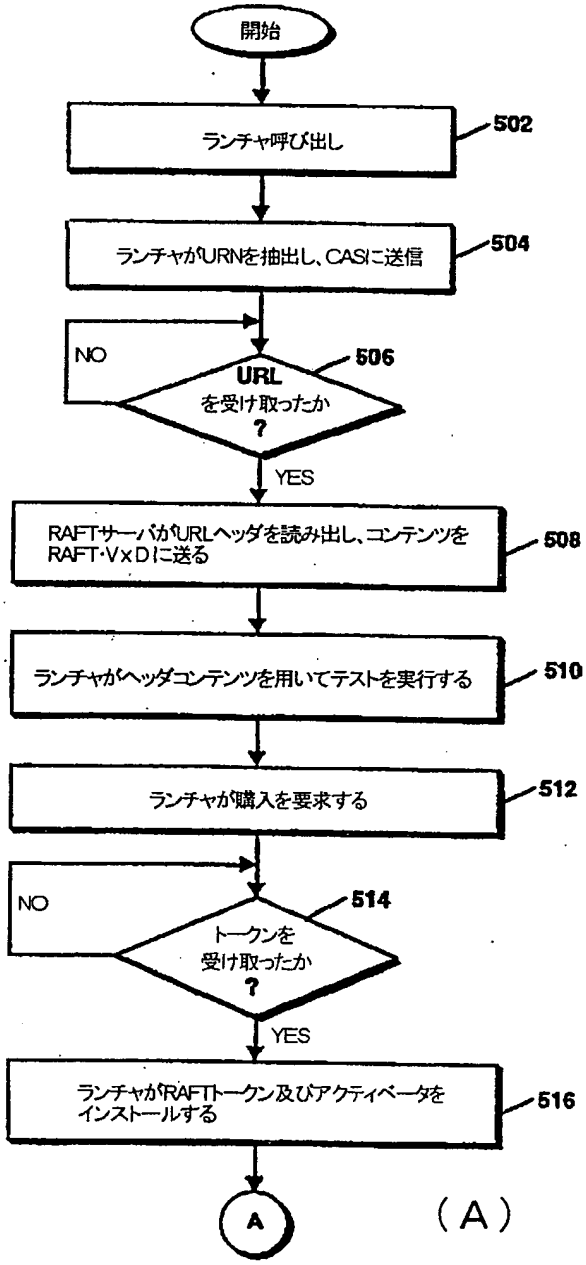

開始
ユーザによるタイトル選択
401
デジタルオッファーによって、SCDPクライアントがブラウザをEコマースシステムに導く
402
ユーザがEコマースシステムとタイトルの購入交渉する
403
Eコマースシステムがランチストリングを生成する
404A
CASがランチストリングにデジタル署名する
404B
SCDPクライアントがランチストリングを受け取り、ランチャモジュールを呼び出す
405B
ランチャが、URN－URL変換のためにURNを提出する
406A
ランチャがURLを受け取り、CASからの購入を要求する
406B
A
（Ａ）

【図４Ｂ】

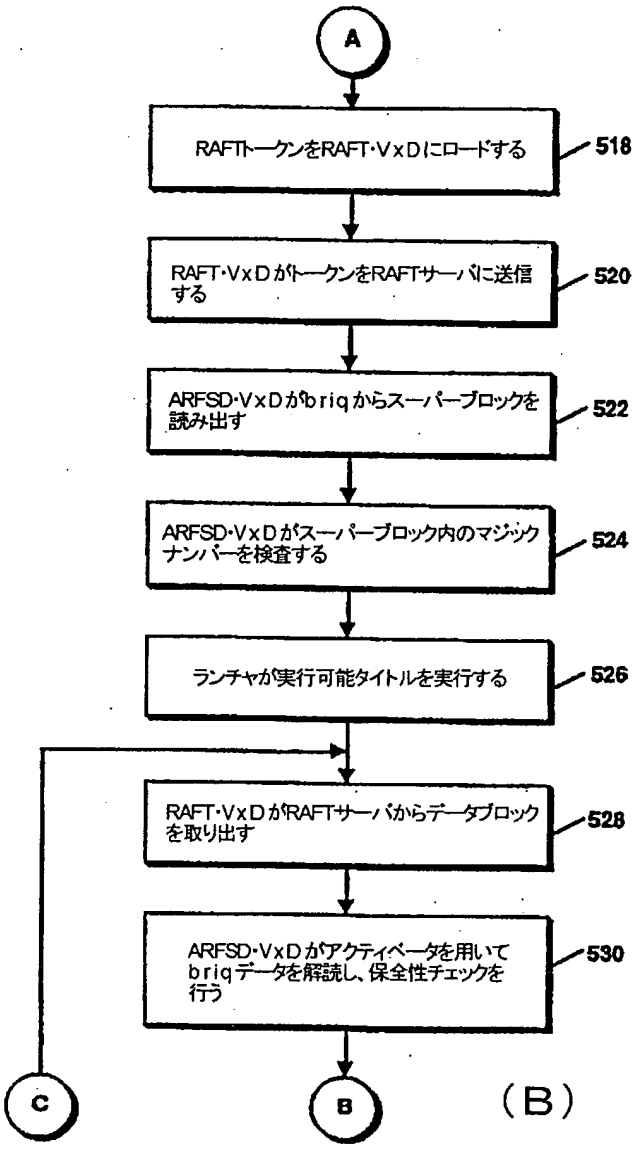

A
CASがランチストリングを検査して、RAFTトークン及びアクティベータをランチャに送る
407
ランチャがタイトルをランチする
408
RAFT VxD がトークンヘッダを読み出す
409
RAFT VxD がトークンをRAFTサーバに送る
410
RAFT VxD がRAFTサーバからタイトルコンテンツを読み出し、ARFSD VxD に送る
411
アクティベータがbriqデータ(タイトル)を解読し、復元解凍する
412
インストール抄録を用いて、SCDPクライアントのローカルオペレーティングシステムによりタイトルが実行される
413
アクティベータがトークン更新を要求する;CASがEコマースシステムに購入を通知する;CASが更新したトークンを発行する
414
終了

（Ｂ）

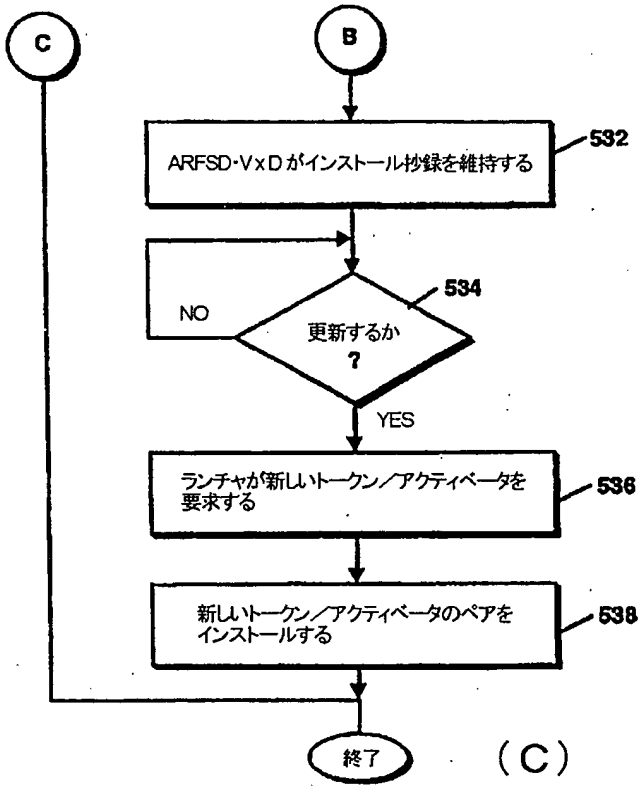
【図５Ａ】


開始
ランチャ呼び出し
502
ランチャがURNを抽出し、CASに送信
504
NO
URL
を受け取ったか
?
506
YES
RAFTサーバがURLヘッダを読み出し、コンテンツを
RAFT・VxDに送る
508
ランチャがヘッダコンテンツを用いてテストを実行する
510
ランチャが購入を要求する
512
NO
トークンを
受け取ったか
?
514
YES
ランチャがRAFTトークン及びアクティベータを
インストールする
516
A
（A）

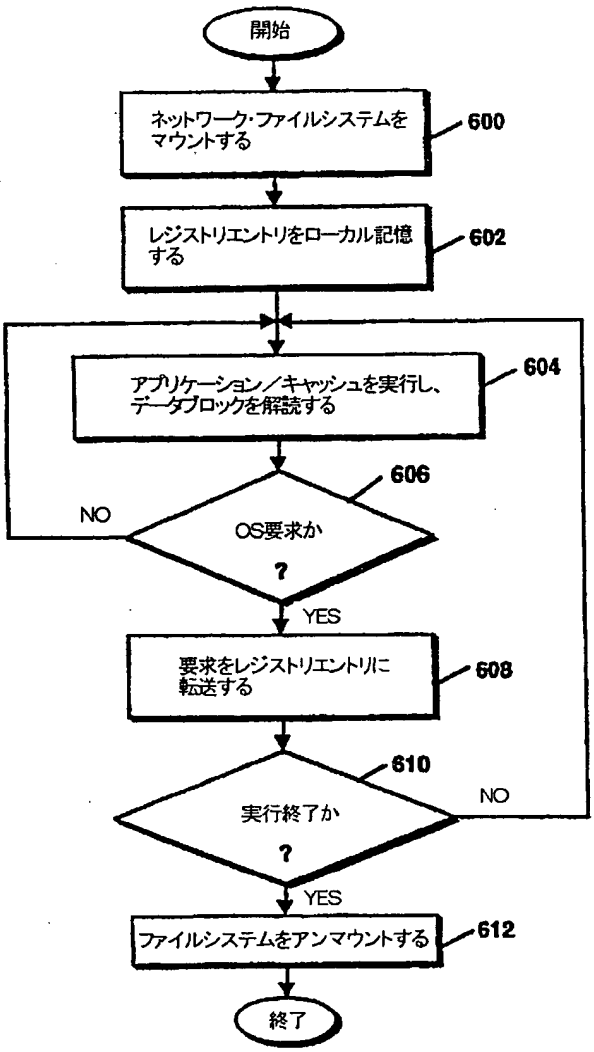
【図５Ｂ】


A
RAFTトークンをRAFT・VxDにロードする
518
RAFT・VxDがトークンをRAFTサーバに送信する
520
ARFSD・VxDがbriqからスーパーブロックを読み出す
522
ARFSD・VxDがスーパーブロック内のマジックナンバーを検査する
524
ランチャが実行可能タイトルを実行する
526
RAFT・VxDがRAFTサーバからデータブロックを取り出す
528
ARFSD・VxDがアクティベータを用いてbriqデータを解読し、保全性チェックを行う
530
C
B
(B)

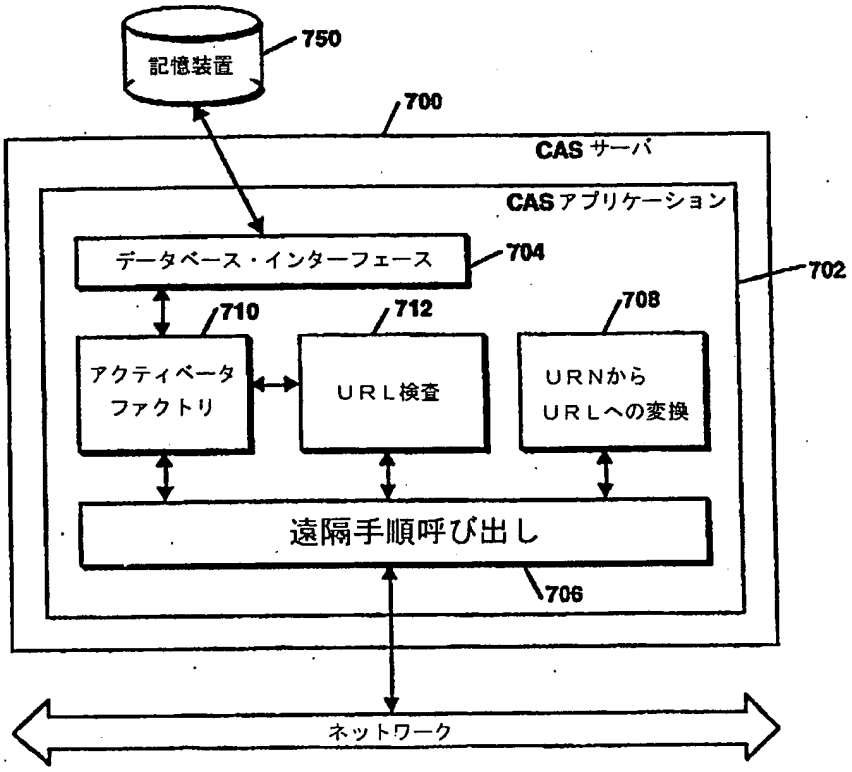
【図５Ｃ】


C
B
ARFSD・VxDがインストール抄録を維持する
532
NO
更新するか
?
534
YES
ランチャが新しいトークン／アクティベータを
要求する
536
新しいトークン／アクティベータのペアを
インストールする
538
終了
(C)

【図６】

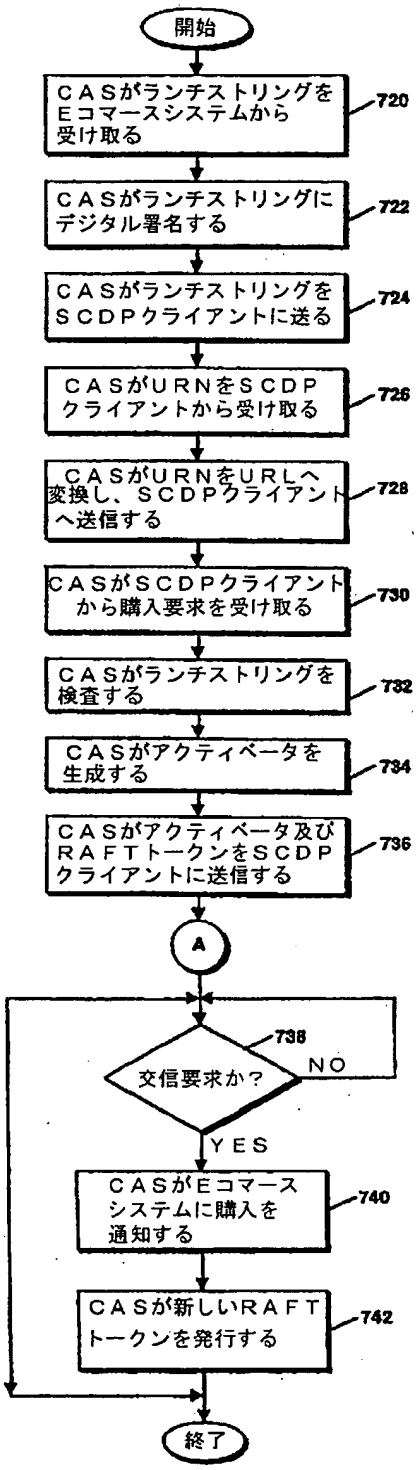

開始
ネットワーク・ファイルシステムをマウントする
600
レジストリエントリをローカル記憶する
602
アプリケーション／キャッシュを実行し、データブロックを解読する
604
606
NO
OS要求か
？
YES
要求をレジストリエントリに転送する
608
610
NO
実行終了か
？
YES
ファイルシステムをアンマウントする
612
終了

【図７Ａ】


記憶装置
750
700
CASサーバ
CASアプリケーション
データベース・インターフェース
704
702
710
712
708
アクティベータ
ファクトリ
URL検査
URNから
URLへの変換
遠隔手順呼び出し
706
ネットワーク

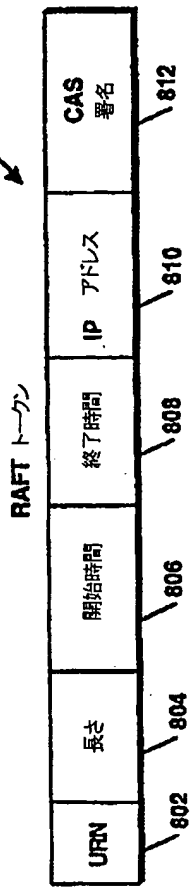
（Ａ）

【図７Ｂ】

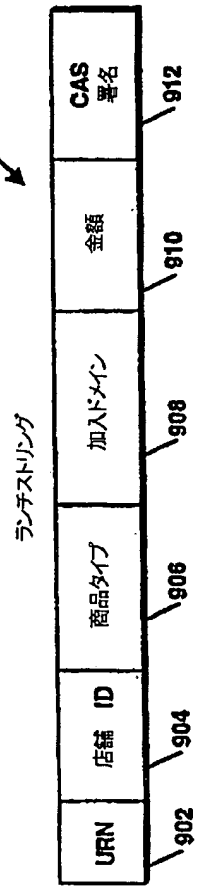

開始
ＣＡＳがランチストリングを
Ｅコマースシステムから
受け取る
720
ＣＡＳがランチストリングに
デジタル署名する
722
ＣＡＳがランチストリングを
ＳＣＤＰクライアントに送る
724
ＣＡＳがＵＲＮをＳＣＤＰ
クライアントから受け取る
726
ＣＡＳがＵＲＮをＵＲＬへ
変換し、ＳＣＤＰクライアント
へ送信する
728
ＣＡＳがＳＣＤＰクライアント
から購入要求を受け取る
730
ＣＡＳがランチストリングを
検査する
732
ＣＡＳがアクティベータを
生成する
734
ＣＡＳがアクティベータ及び
ＲＡＦＴトークンをＳＣＤＰ
クライアントに送信する
736
A
738
交信要求か？
NO
ＹＥＳ
ＣＡＳがＥコマース
システムに購入を
通知する
740
ＣＡＳが新しいＲＡＦＴ
トークンを発行する
742
終了

（Ｂ）

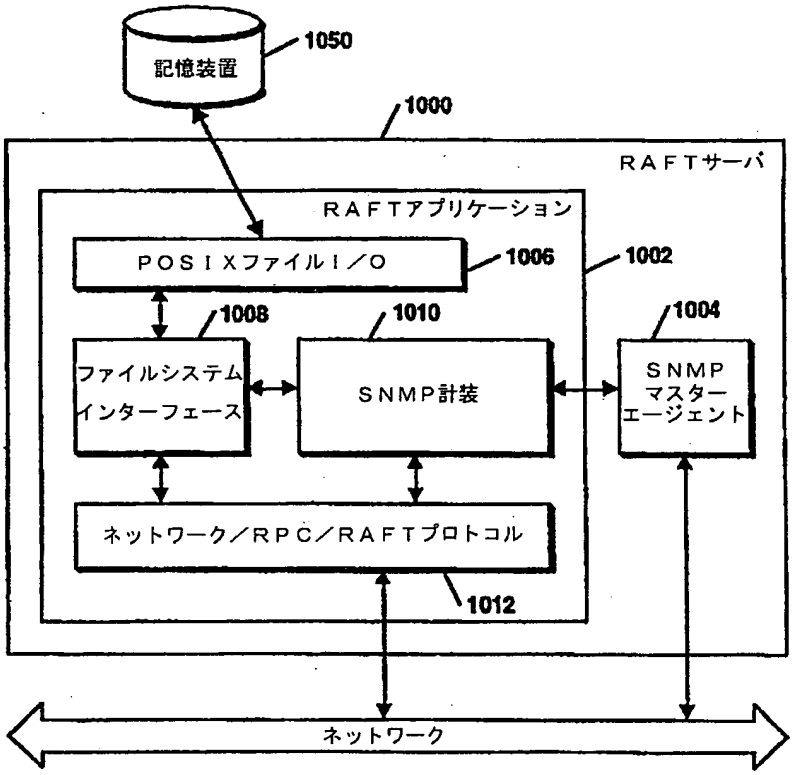
【図８】


800
RAFT トークン
URN
長さ
開始時間
終了時間
IP アドレス
CAS 署名
802
804
806
808
810
812

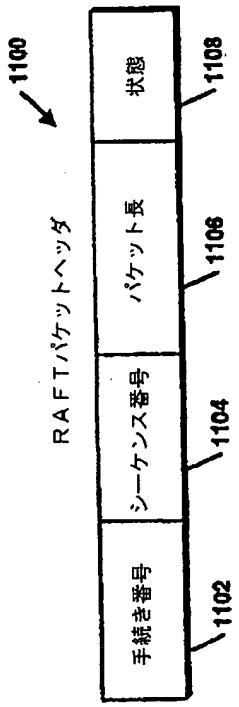
【図９】


900
ランチストリング
URN
902
店舗 ID
904
商品タイプ
906
加入ドメイン
908
金額
910
CAS 署名
912

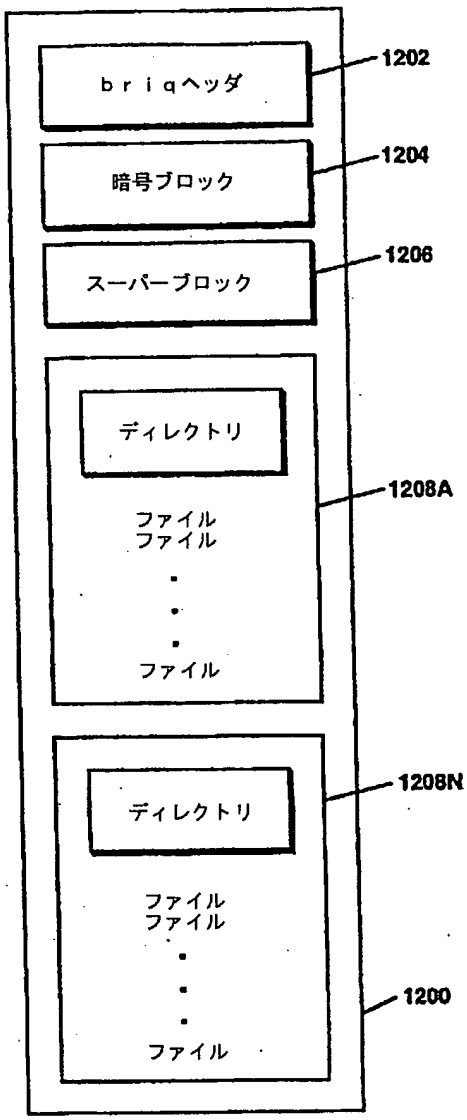
【図１０】


記憶装置
1050
1000
RAFTサーバ
RAFTアプリケーション
POSIXファイルI／O
1006
1002
1008
1010
1004
ファイルシステム
インターフェース
SNMP計装
SNMP
マスター
エージェント
ネットワーク／RPC／RAFTプロトコル
1012
ネットワーク

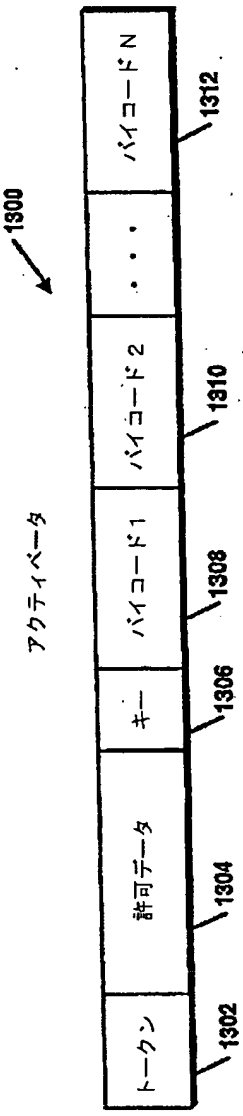
【図１１】


1100
RAFTパケットヘッダ
状態
1108
パケット長
1106
シーケンス番号
1104
手続き番号
1102

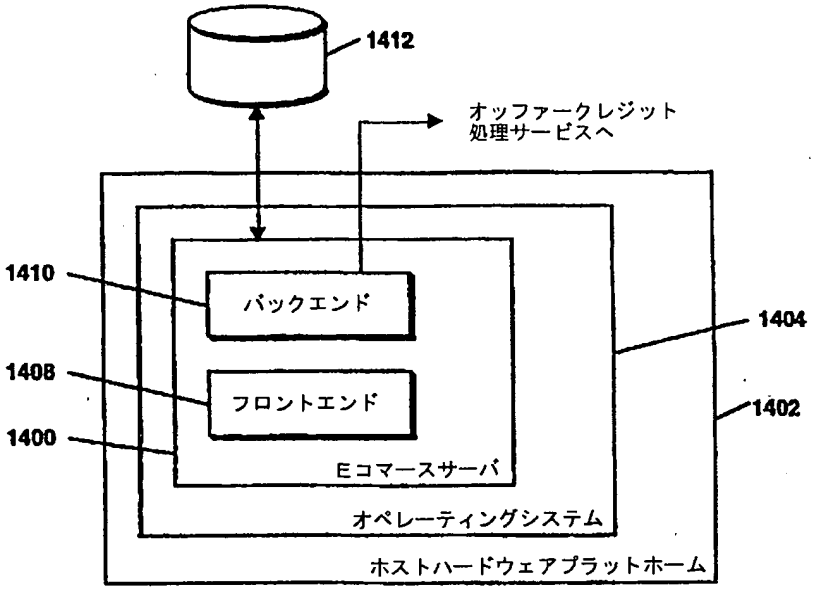
【図１２】


ｂｒｉｑヘッダ
1202
暗号ブロック
1204
スーパーブロック
1206
ディレクトリ
ファイル
ファイル
ファイル
1208A
ディレクトリ
ファイル
ファイル
ファイル
1208N
1200

【図１３】


1300
アクティベータ
トークン
1302
許可データ
1304
キー
1306
バイコード1
1308
バイコード2
1310
・・・
バイコードN
1312

【図１４】


1412
オッファークレジット
処理サービスへ
1410
バックエンド
1404
1408
フロントエンド
1402
1400
Eコマースサーバ
オペレーティングシステム
ホストハードウェアプラットホーム

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inter xnal Application No
PCT/US 99/27113

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F9/45

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 99 45491 A (NUVOMEDIA INC) 10 September 1999 (1999-09-10) abstract page 1, line 7 - line 11 page 2, line 31 -page 3, line 4 page 4, line 9 - line 27 page 5, line 28 - line 32 page 7, line 2 - line 6 page 7, line 25 - line 31 page 15; claim 1 — -/—	1,5

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 May 2000	07/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Adkhis, F

Form PCT/ISA/210 (second sheet) (July 1992)

page 1 of 2

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/US 99/27113

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	RUBIN A D: "Secure distribution of electronic documents in a hostile environment" COMPUTER COMMUNICATIONS,NL,ELSEVIER SCIENCE PUBLISHERS BV, AMSTERDAM, vol. 18, no. 6, 1 June 1995 (1995-06-01), pages 429-434, XP004032475 ISSN: 0140-3664 abstract page 430, right-hand column, line 9 - line 43 page 431, left-hand column, line 35 - line 57	1-21

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inte. onal Application No
PCT/US 99/27113

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9945491 A	10-09-1999	WO 0021239 A	13-04-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(51)Int.Cl.[7]	識別記号	F I		テーマコード(参考)
G06F 17/30	120	G06F 9/06	660C	
			660G	

(31)優先権主張番号 09／311，923
(32)優先日 平成11年5月12日(1999. 5. 12)
(33)優先権主張国 米国（US）
(31)優先権主張番号 09／310，229
(32)優先日 平成11年5月12日(1999. 5. 12)
(33)優先権主張国 米国（US）
(31)優先権主張番号 09／439，906
(32)優先日 平成11年11月12日(1999. 11. 12)
(33)優先権主張国 米国（US）
(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), AU, CA, CN, JP, KR, SG, ZA

(72)発明者 エイチン マーク ダブリュー
アメリカ合衆国 マサチューセッツ州 02144 サマービル シャープ331 ハイランド アベニュー 411エー
(72)発明者 ロストチェック デービッド ジェイ
アメリカ合衆国 マサチューセッツ州 02474 アーリントン ブルックデール ロード 9

Fターム(参考) 5B017 AA03 BA07 BB10 CA15
5B075 KK43 KK54 NK04 PQ05
5B076 FB01
5B082 EA12 GA11 HA05